An Exploratory Study On Systems Security And Hacker Hiring

Siew H. Chan, (Email: Siew.Chan@umb.edu), University of Massachusetts, Boston
Lee J. Yao, La Trobe University, Australia

Abstract

We conducted an exploratory study to enhance understanding on systems security and hacker hiring. Increased understanding on these issues will assist firms in developing effective guidelines for mitigating problems associated with potential attacks and in designing recruitment procedures for hiring hackers. Specifically, we examine the impact of corporate security policies on perceived systems security; the impact of internal (external) systems security audits on perceived systems security; and the willingness of firms in hiring hackers.

Introduction

The information age has created an environment whereby information is a key asset and information security is a strategic variable that helps firms gain a competitive advantage (Gordon, Loeb, & Lucyshyn, forthcoming). Despite the importance of information security, effective measures backed by appropriate budgetary funding have not been forthcoming to protect the information that resides on systems. In a study conducted by Cap Gemini Ernst and Young, 63% of 265 chief financial officers indicated that their work was affected by inadequate budgeting, forecasting, and decision support systems (Songini, 2002). A security report by Forrester Research suggested that lack of substantial information on a quantifiable measure of return on security investment has led many chief information officers to reduce the amounts spent on core systems security. In an environment of limited resources, this diversion of funds points to a steady shrinking pool of funds available for covering the vulnerabilities of internally automated business processes (www.ecommercetimes.com). Many firms, particularly financial institutions, are now outsourcing their operations to mitigate their budget problems. These firms face the risk of security breaches if their hosting companies do not implement sound security policies and procedures (Hoffman, 2002). Security breaches can result in adverse economic consequences such as negative reputation, higher costs to detect or correct the breaches, and potential legal liability (Campbell, Gordon, Loeb, & Zhou, forthcoming). A report on www2.cio.com predicted that more than 75% of Global 2000 companies would adopt enterprise-wide information security policies. Chief information officers who link security policies with enterprise-wide information policies have a better chance of earning the trust and respect of their colleagues and in achieving better communication of shared responsibility for safeguarding information assets (www2.cio.com). Firms should also provide security training for systems users to increase awareness on the impact that a security breach could have on the entire business operation (Locke & Hartley, 2001).

However, firms are expected to increase spending to comply with the requirements of the Sarbanes-Oxley Act (SOA). AMR Research projected that firms would spend about $5.5 billion in 2004 to comply with SOA (www.dmreview.com, January 2004). Software packages (e.g., IDS Scheer's ARIS Sarbanes-Oxley Audit Manager, Preventsys Network Audit and Policy Assurance System, HandySoft's Sarbanes-Oxley Accelerator, SAP Compliance Management for Sarbanes-Oxley Act, SAS Corporate Compliance for Sarbanes-Oxley, and Vignette V7) are now available to help firms achieve compliance with SOA. Besides chief executive officers and chief financial officers, chief information officers are also affected by SOA because assurance of compliance is provided by the systems that contain the financial information (Imhoff, 2004). Since IT plays a significant role in the development, operation, and maintenance of information systems that contain the financial results of firms, project steering committees formed to achieve compliance with SOA should include the IT function (www.dmreview.com, December 2003). Despite the importance of the IT function, The Hackett Group, an Answerthink company,

reported that about 50% of the firms surveyed did not have IT representation on their steering committees (www.dmreview.com, December 2003).

Prior research (e.g., Gordon & Loeb 2002; Gordon et al., forthcoming; Campbell et al., forthcoming) use economics as a framework to examine variables such as return on investment in information security and the economic cost of publicly announced information security breaches. Gordon et al. (forthcoming) suggested that it may be rational to take a "wait-and-see" approach toward spending some of the funds earmarked for information security because of the uncertain occurrence of security breaches. Since substantial amounts of money are invested in information security activities, it is not surprising that chief financial officers are demanding a rational approach to such expenditures; this includes increased adoption of return on security investments as a measure to capture the cost-benefit aspect of information security (Gordon & Loeb, 2002). Campbell et al. (forthcoming) reported a significant negative market reaction to security breaches involving unauthorized access to confidential information but no market reaction toward breaches that did not involve confidential information. These findings suggest that the economic consequences of a security breach vary in accordance with the nature of the assets compromised by the breach (Campbell et al., forthcoming). We add to the stream of research developed by Gordon and Loeb and their colleagues by examining the issue of systems security from a behavioral perspective.

We conducted an exploratory study to enhance understanding on systems security and hacker hiring. Increased understanding on these issues will assist firms in developing effective guidelines to mitigate problems associated with potential attacks and in designing recruitment procedures for hiring hackers. We examine the impact of corporate security policies on perceived systems security; the impact of internal and external systems security audits on perceived systems security; and the willingness of firms in hiring hackers. We mailed our research instrument to 998 Information Week subscribers and received 131 usable responses for a response rate of about 13%. Our results showed that IT professionals felt that firms with corporate security policies were less vulnerable to attacks by external parties; had intrusion detection systems that were more successful at detecting intrusions; had more secure systems; and viewed systems security as an important issue. However, existence of a corporate security policy did not have an impact on perceived vulnerability of systems to attacks by internal parties. We also found that firms with more frequent internal systems security audit were perceived to (a) be more successful at detecting intrusions; (b) have more secure systems; and (c) be less vulnerable to attacks by internal parties. Although firms with more frequent external systems security audit were perceived to be more successful at detecting intrusions, they were not perceived to have more secure systems or less vulnerable to attacks by external parties. Finally, we found that white hat hackers were more likely to be hired when they hacked for intrinsic reasons, and reformed hackers were more likely to be hired when they hacked for extrinsic reasons.

The next section discusses the propositions posed in our study. The third section explains the research method used to address our propositions. The statistical results are presented in the fourth section. Finally, our concluding remarks and suggestions for future research are discussed.

Propositions

A 2002 survey conducted by the Computer Security Institute Computer Crime and Security indicated that more than half of the databases have been breached in some way; resulting in estimated losses of almost $4 million on average for each breach (Nevins, 2003). Computer crimes such as sabotage, embezzlement, and computer fraud can have a tremendous impact on business operations. Survey results showed that chief information officers and IT managers lacked confidence in existing computer security practices (Hoffman, 2002). Despite the importance of corporate security policies, a survey conducted by Datapro Information Services Group showed that 40% of U.S. firms did not have a corporate security policy[1] (Anthes, 1995).

A corporate security policy should be in place to improve security (Locke & Hartley, 2001) and "to address issues pertaining to system access controls, data confidentiality/privacy, and data integrity" (e-Business Advisor, 1998, p. S6). This document should state clearly the policies and procedures for protecting systems and the

[1] We provide an updated figure on the percentage of firms that currently have corporate security policies.

information that resides on these systems. Sound corporate security policies can help firms attain their goals with respect to security of their systems (Packer, 2001). Firms can implement corporate security policies as a strategy to send a message to potential investors that they view systems security seriously. This action might be taken to create a favorable stock market reaction to increase stock prices. Currently, limited research is available to help us understand whether IT professionals feel that their firms' corporate security policies are effective in preventing security breaches. These individuals may believe that firms with corporate security policies are less vulnerable to attacks by internal and external parties. On the other hand, they may feel that corporate security policies provide firms with a plan for detecting intrusions, leading to the perception that systems are secure. This leads to the first proposition:

Proposition 1: Firms with corporate security policies (a) are less vulnerable to attacks by internal parties; (b) are less vulnerable to attacks by external parties; (c) are more successful at detecting intrusions; (d) have more secure systems; and (e) view systems security as an important issue.

Since attacks are not limited to external parties, firms must prepare themselves for attacks by internal parties such as disgruntled employees or contractors who might cause damage to their systems for fiduciary gains or to steal data. A Michigan State University survey reported that nearly every large U.S. firm had been a victim of computer crimes and many of these crimes were committed repeatedly and primarily by employees (Anthes, 1995). "Law enforcement experts now estimate that more than half of all identity theft cases are committed by employees with access to large financial databases" (Nevins, 2003). Gartner estimated that internal employees conducted 70% of the security breaches and this figure was not far off from 95% of the intrusions committed by external parties that led to substantial financial losses (Nevins, 2003). A database administrator with unrestricted access to a database could breach security and steal confidential business, financial, or customer data (Nevins, 2003). A global investment bank conducted an internal audit and found that 12 database administrators had unlimited access to highly confidential databases and more than 100 employees had access to its database's operating systems (Nevins, 2003). The internal audit also revealed weaknesses in the bank's backup process; specifically, information was subject to breaches in the event of a stolen or lost data tape. As a result, the chief information officer decided that the bank had to protect its confidential information from internal or external threats (Nevins, 2003). In another case, an internet service provider was shut down for five days after a former employee engaged in a damaging security violation (Callaway, 1996).

Chief information officers should ensure that usage rules and audit trails are in place for systems that contain the financial information for corporate reporting (www.dmreview.com, December 2003). Security experts can be retained to conduct regular internal audits of systems to ensure that they are in compliance with the firms' corporate security policies. The Information Systems Audit and Control Foundation developed the Control Objectives for Information Related Technologies (COBIT), "a framework of generally applicable information systems security and control practices for IT control" (Romney & Steinbart, 2003, p. 196-197). COBIT is designed to be consistent with the Committee of Sponsoring Organizations (COSO[2]) internal control model. Proper audit procedures and security programs can be implemented to prevent security breaches (Nevins, 2003). Frequent internal system audits might provide firms with a sense of security in that they may feel that their systems are more successful at detecting intrusions. Internal parties might also be discouraged from launching an attack against their firms' systems if they feel that the possibility of their activity being discovered is high. As such,

Proposition 2a: Firms that conduct more frequent internal systems security audits (a) are more successful at detecting intrusions; (b) have more secure systems; and (c) are less vulnerable to attacks by internal parties.

Independent contractors can be hired to conduct an independent review and assessment of security of systems. Security experts may review policies and procedures, disaster recovery plans, insurance policies, access logs, and other security issues. Although IT professionals may feel that more frequent external audits may result in increased success at detecting intrusions, it is uncertain as to whether more frequent external audits would lead to the perception that the systems are more secure and less vulnerable to attacks by external parties. It is conceivable that

[2] COSO comprises several organizations including the American Accounting Association, American Institute of Certified Public Accountants, the Institute of Internal Auditors, the Institute of Management Accountants, and the Financial Executives Institute.

firms may have control over the behaviors of internal employees; however, they do not have control over the behaviors of external parties. Thus,

Proposition 2b: Firms that conduct more frequent external systems security audits are more successful at detecting intrusions; however, their systems may not be more secure or less vulnerable to attacks by external parties.

Firms might consider hiring hackers as part of their security control teams to combat information security breaches. Some believe that it takes a thief to catch a thief and that it may be appropriate to use a reformed hacker to simulate an attack (Bennett, 2002). The question of whether former hackers should be hired is a controversial one. Some firms prefer to play it safe than to risk hiring former hackers. *Computer Insider*, a newsletter for hackers, estimated that about 900 hackers were hired in the last four years by organizations that they once targeted. A survey conducted by Computer Security Institute and Federal Bureau of Investigation showed that 68% of the security professionals indicated that they would not hire reformed hackers, 15% said they would, and 17% were unsure. Although preventive controls such as background checks are desirable in the hiring process, it is difficult to determine whether former hackers are truly reformed and that they would not engage in activities to hack the systems of their prospective employers. A government agency hired a hacker to do research on its vulnerabilities. The hacker was fired when he reported only one or two vulnerabilities each week and made these vulnerabilities known to his friends (Business Wire, 2000). In another instance, upon interviewing a former hacker, a company found that the hacker still possessed a strong hacker mentality and had no choice but to disqualify him from further consideration for a job (Callaway, 1996). On the other hand, it is possible that some hackers are reformed. Kevin Mitnick, who was convicted of computer crimes in 1996 and released in 2000, subsequently became the president of a security consulting firm, Defensive Thinking. Mitnick maintained that he was reformed and that his skills were of value to the IT profession (Savage, 2003). Another reformed hacker became a chief security officer of a security products company in Westboro (Weinstein, 2002). "Kuji", a former hacker, worked as a security consultant and was selected to head the marketing campaigns of some reputable companies (Cushing, 2001). In another instance, a hacker received job offers from several German companies desperate for his expertise in beefing up their security systems from external threats after he successfully created a negative balance in a German bank account (Cushing, 2001).

Ethical or "white hat" hackers must be distinguished from unethical or "black hat" hackers and the underlying motivation for hacking should be understood before effective corporate security policies can be implemented to counteract potential attacks. A person's underlying motivation for hacking is a key distinguishing factor between a "white hat" and "black hat" hacker. "White hat" hackers conduct penetration tests to identify system vulnerabilities and inform the owners of these problems (Cushing, 2001). These individuals are likely former hackers who have moved on to become security professionals (Thomas, 2002). One security manager hired a hacker after the latter gave him a web address that showed the firm's customer names, addresses, phone numbers, and credit card numbers (Thurman, 2001). This hacker found that the application programming interface was not configured properly. The security manager might have hired this hacker because he hacked for his interest in security rather than for malicious intentions. Thus, a hacker's intentions may be the determining factor in a security manager's decision about whether a hacker should be hired. In contrast, "black hat" hackers pursue activities with the intention of causing damage to systems or for fiduciary gains. For example, Western Union was forced to shut down its website for five days after the card numbers of more than 15,000 customers were stolen by hackers (Hopper, 2001).

Individuals may engage in hacking for intrinsic (e.g., interest, challenge, curiosity, or fun) or extrinsic (e.g., recognition of achievements by social groups, identification with social groups, prestige, financial gains, or political motives) reasons. An example of hacking for intrinsic reasons was a case where one hacker indicated that he hacked because of the thrill and enjoyment that he derived from engaging in such an activity (Mulhull, 1999). Individuals may also hack for financial gains. A group of hackers stole one million credit card numbers over the Internet, revealed the break-in, posted the credit card numbers on the Internet, and offered to provide "security" services for a fee (Wallace, 2001). In another case, a Russian hacker stole more than 55,000 credit cards from creditcards.com (a website that processed transactions for online merchants) and posted about 25,000 credit card numbers online when his demand for $100,000 was ignored (Hopper, 2001). However, limited research is available to help us understand

whether a person's reasons for hacking would have an impact on a firm's willingness in hiring her. A hacker who hacks for intrinsic reasons such as interest, challenge, curiosity, or fun may be perceived to be less likely to hack for malicious intentions. This individual is mostly likely a white hat hacker. Firms may be more willing to hire white hat hackers because these individuals are less likely to cause harm or damage to their systems. Another group of hackers; specifically the reformed hackers, may be hired if they hack for extrinsic reasons. Individuals who hack for extrinsic reasons are predicted to be discouraged by prosecution, conviction, and imposition of stringent punishment. In the absence of extrinsic reasons for hacking, the likelihood that these individuals are truly reformed might increase and this might in turn increase the likelihood of their being hired. Finally,

Proposition 3a: Firms are more willing to hire white hat hackers if they hack for intrinsic reasons.

Proposition 3b: Firms are more willing to hire reformed hackers if they hack for extrinsic reasons.

Research Method

Participants

We obtained a list of Information Week subscribers from IDG Communications. We sent our instrument to 998[3] subscribers. Our list included subscribers with a job title of chief information officer or chief technology officer and a job function in security. This group of IT professionals was selected because we felt that they would be appropriate participants for answering the questions in our research instrument. We used the 50th percentile to create two groups of early and late respondents. We performed ANOVA tests on the dependent variables but did not find any significant differences between the early and late respondents. We received 131 usable responses for a response rate of about 13%[4]. Our response rate was comparable to the response rates obtained in prior research. Trahan and Gitman (1995) had 12% using chief financial officers; Graham and Harvey (2001) had 9% using chief financial officers; Nelson, Elliott, and Tarpley (2002) had 16% using experienced auditors; and Hodge, Martin, and Pratt (Working paper) had 25% using alumni at a major business school.

Table 1 contains the demographics of our participants.

Research Instrument

Our research instrument consisted of four parts. Part I contained questions about security of systems in the participants' firms. Part II collected data on the participants' perceptions about hackers. Data on the participants' firms and demographics were collected in Parts III and IV respectively. The questions were in the form of a 7-point Likert scale and checked options. Participants also entered data such as percentages and numbers. We pretested and improved our instrument based on valuable comments received from IT professionals and colleagues at our universities. We included some definitions in our instrument to ensure accurate data collection. Specifically, we defined internal parties as employees and external parties as non-employees. We described a white hat hacker as a person dedicated to improving systems security by seeking out flaws and finding ways to repair them. We defined a reformed hacker as one who no longer hacked to exploit for personal gains (Thomas, 2002).

Data Analysis And Results

Independent Variables

The independent variables are: existence of a corporate security policy, frequency of internal systems security audit, frequency of external systems security audit, intrinsic reasons for hacking, and extrinsic reasons for hacking. The first independent variable has two levels: presence or absence of a corporate security policy.

[3] We had 1,000 names initially; however, the addresses of two subscribers were incomplete. Twelve mails were returned to us as undeliverable.
[4] In addition, weak economic conditions led to losses of several IT positions; as a result, our mails might not have reached all potential subscribers.

Table 1
Demographics of Participants

Age:	45 (mean)
Gender:	114 males; 10 females
Education:	
High school diploma	10%
Bachelor's degree	55%
Master's degree	26%
Income	between $75,000 and $100,000 (median)
Professional Experience	20 years (mean)
Professional Certifications:	
Operating system	38%
Network	36%
Hardware	24%
Application development	22%
Communications	17%
Database	16%
Security	14%
Internet/Web	10%
Helpdesk	9%
Trainer	9%
ERP	7%
Wireless	5%
Others	5%

*8 participants did not indicate their age and gender; 7 did not indicate their highest education attained, current employment status, and years of professional experience; and 16 did not provide information on their income.

Frequency of internal (external) systems security audit has the following five levels: once a month, once every three months, once every six months, once a year, and rarely. The intrinsic reasons and extrinsic reasons constructs are derived from a set of variables. Interest, challenge, curiosity, and fun are grouped to form the intrinsic reasons for hacking construct. The correlation coefficients for these variables ranged between 0.56 and 0.69 (p=0.000) and the reliability coefficient was 0.86 (see Exhibit 1). Recognition of achievements by the hacking community, identification with the hacking community, financial gains, prestige, and political motives were grouped to derive the extrinsic reasons for hacking construct. The correlation coefficients for these items ranged between 0.36 and 0.73 (p=0.000) and the reliability coefficient was 0.85 (see Exhibit 2).

Dependent Variables

The dependent variables include (1) perceived vulnerability of systems to attacks by internal parties; (2) perceived vulnerability of systems to attacks by external parties; (3) the extent of success of intrusion detection systems at detecting intrusions; (4) security of systems; (5) the importance of systems security; (6) the likelihood that white hat hackers are hired; and (7) the likelihood that reformed hackers are hired. These variables were scored on a 7-point scale with 1=not at all and 7=to a great extent.

Results

Since the independent variables in Propositions 1, 2a, and 2b were categorical in nature, ANOVA was used to test these propositions. Regression was used to test Propositions 3a and 3b because the independent variables were continuous in nature. Table 2 shows the results of our propositions. Proposition 1 states that firms with corporate security policies are less vulnerable to attacks by internal parties; are less vulnerable to attacks by external parties; are more successful at detecting intrusions; have more secure systems; and view systems security as an

Exhibit 1
Reliability Analysis of Intrinsic Reasons Construct

	Mean	Std Dev	Cases
Interest	3.9695	1.8478	131.0
Challenge	3.4504	1.7941	131.0
Curiosity	4.7328	1.7401	131.0
Fun	4.4580	1.7900	131.0

Correlation Matrix

	Interest	Challenge	Curiosity	Fun
Interest	1.0000			
Challenge	0.5587	1.0000		
Curiosity 0.6027	0.5489	1.0000		
Fun	0.5950	0.6443	0.6891	1.0000

Label	Description of Item
Interest	If a hacker hacks for the sake of *interest or enjoyment*, do you think that the consequences (in Question 1, Part II) would discourage the hacker from hacking?
Challenge	If a hacker hacks for the sake of *challenge*, do you think that the consequences (in Question 1, Part II) would discourage the hacker from hacking?
Curiosity	If a hacker hacks for the sake of *curiosity*, do you think that the consequences (in Question 1, Part II) would discourage the hacker from hacking?
Fun	If a hacker hacks for *fun*, do you think that the consequences (in Question 1, Part II) would discourage the hacker from hacking?

important issue. About 70% of our participants indicated that their firms had a corporate security policy[5]. These individuals felt that their firms were less vulnerable to attacks by external parties (p=0.051), their firms' intrusion detection systems were more successful at detecting intrusions (p=0.025), their firms' systems were more secure (p=0.016), and their firms viewed systems security as an important issue (p=0.000). Overall, our results provide support for Proposition 1 except for the finding that corporate security policies did not have an impact on perceived vulnerability of firms to attacks by internal parties.

Proposition 2a suggests that firms with more frequent internal systems security audits are more successful at detecting intrusions; have more secure systems; and are less vulnerable to attacks by internal parties. Proposition 2a is supported at p=0.004, p=0.003, and p=0.000 respectively. Proposition 2b proposes that firms with more frequent external systems security audits are more successful at detecting intrusions; however, their systems may not be more secure or less vulnerable to attacks by external parties. Our participants felt that more frequent external systems security audits led to more successful intrusion detection (p=0.044). However, more frequent external systems security audits did not have a significant impact on perceived systems security and vulnerability of these systems to attacks by external parties. Proposition 3a examines whether IT professionals are more willing to hire white hat hackers if they hack for intrinsic reasons. This proposition is supported at p=0.005. Proposition 3b looks at whether IT professionals are more willing to hire reformed hackers if they hack for extrinsic reasons. The regression results provide marginal support for Proposition 5 (p=0.091) while the ANOVA[6] results support this proposition at p=0.050.

[5] One participant did not indicate whether her firm had a corporate security policy.
[6] We used the 50th percentile to create two levels of the extrinsic reasons for hacking construct.

Exhibit 2
Reliability Analysis of Extrinsic Reasons Construct

	Mean	Std Dev	Cases
Recog	3.4275	1.8812	131.0
Identify	3.3893	1.7390	131.0
Gains	3.5420	2.0048	131.0
Prestige	3.6107	1.8169	131.0
Politics	2.8397	1.8306	131.0

Correlation Matrix

	Recog	Identify	Gains	Prestige	Politics
RECOG	1.0000				
IDENTIFY	0.7270	1.0000			
GAINS	0.3746	0.4112	1.0000		
PRESTIGE	0.7130	0.6521	0.5061	1.0000	
POLITICS	0.3640	0.4330	0.6128	0.4506	1.0000

Label	Description of Item
Recog	If a hacker hacks for *recognition of achievement by the hacking community*, do you think that the consequences (in Question 1, Part II*) would discourage the hacker from hacking?
Identify	If a hacker hacks to *identify or associate with the hacking community*, do you think that the consequences (in Question 1, Part II*) would discourage the hacker from hacking?
Gains	If a hacker hacks for *financial gains*, do you think that the consequences (in Question 1, Part II*) would discourage the hacker from hacking?
Prestige	If a hacker hacks for the sake of *prestige or status*, do you think that the consequences (in Question 1, Part II*) would discourage the hacker from hacking?
Politics	If a hacker hacks for *political motives*, do you think that the consequences (in Question 1, Part II*) would discourage the hacker from hacking?

*What kinds of consequences do you think would discourage a hacker from hacking? (Check all applicable options: imprisonment, fine, censure by the hacker's profession, censure by the IT community, ban on future access to systems, loss of job, publicity of a hacker's activity, publicity of a hacker's identity, nothing will stop a hacker from hacking)

Additional Analyzes

Additional analyzes reveal that 36% of our participants indicated that their firms' systems had been intruded previously[7]. With respect to the question about how frequent their firms' systems were being intruded, 80% indicated a 3 or lower on a Likert scale from 1 to 7 with 1=rarely and 7=very often. 85% indicated a 3 or lower[8] on the extent of damage to their firms' systems, and 94% indicated a 3[9] or lower on the extent of their firms' financial losses (based on their knowledge of the most serious hacking incident). The industries that our participants worked in included manufacturing; information; professional, scientific, and technical services; education services; healthcare and social assistance; public administration; etc. The median number of employees in our participants' firms was 139.[10] In the year 2002, our participants' firms had revenues of $23 million[11] and total assets of $5 million[12]. Their firms invested about $20,000 in systems security each year[13].

[7] They were told to skip the subsequent three questions if they reported that their firms' systems had not been intruded previously.
[8] Likert scale from 1 to 7 with 1=not at all and 7=to a great extent
[9] Likert scale from 1 to 7 with 1=not at all and 7=to a great extent
[10] The median was used because of the wide range of number of employees; that is, from 1 to 300,000. Five participants did not indicate the number of employees in their firms.
[11] The median was used because revenues ranged from $10,000 to $250 billion. 34% did not indicate their firms' revenues for 2002.
[12] The median was used because total assets ranged from $7,000 to $100 billion. 68% did not indicate their firms' total assets for 2002.
[13] The median was used because the amounts invested in systems security ranged from $500 to $1.5 billion. 43% did not indicate the amounts invested in systems security.

About 23% of our participants indicated that their firms' budgets for systems security increased after September 11, 2001; the mean budget increase was 25%. 73% stated that their firms' budgets remained unchanged after September 11, 2001. 11% reported that the current economic condition led to a decrease in their firms' budgets for systems security; the mean budget decrease was 38%. 79% said that the current economic condition did not have an impact on their firms' budget for systems security. 25% indicated that their firms' budgets for systems security for the year 2002 increased compared to the budgets for the previous year; the mean increase was 18%. 60% reported that their firms' budgets remained unchanged during this period.

Exhibit 3 presents the questions for our independent and dependent variables.

Exhibit 3

Independent Variables

1. Does your firm have a corporate security policy for its information systems? (Yes/No)
2. How often does your firm conduct an internal security audit of its information systems? (once a month, once every three months, once every six months, once a year, rarely, others (please specify: _____))
3. How often does your firm conduct an external security audit of its information systems? (once a month, once every three months, once every six months, once a year, rarely, others (please specify: _____))
4. Intrinsic Reasons Construct (see Exhibit 2)
5. Extrinsic Reasons Construct (see Exhibit 3)

Dependent Variables

1. Is information systems security an important issue in your firm?
2. Do you think that your firm's intrusion detection systems are successful at detecting intrusions before the intruders could cause any damage to your firm's information systems?
3. How secure do you think are your firm's information systems?
4. How vulnerable are your firm's information systems to attacks by an internal party (e.g., an employee)?
5. How vulnerable are your firm's information systems to attacks by an external party (e.g., non-employees)?
6. Would you hire a "white hat" hacker (i.e., a hacker dedicated to improving system security by seeking out flaws and finding ways to repair them)?
7. Would you hire a "reformed" hacker (i.e., a hacker who claims that s/he no longer hacks to exploit for personal gains)?

*The dependent variables were based on a 7-point scale with 1=not at all and 7=to a great extent.

Concluding Remarks

Summary

Our findings showed that IT professionals felt that firms with corporate security policies were less vulnerable to attacks by external parties; had intrusion detection systems that were more successful at detecting intrusions; had more secure systems; and viewed systems security as an important issue. However, existence of a corporate security policy did not have an impact on perceived vulnerability of systems to attacks by internal parties. We also found that firms with more frequent internal systems security audit were perceived to (a) be more successful at detecting intrusions; (b) have more secure systems; and (c) be less vulnerable to attacks by internal parties. Although firms with more frequent external systems security audit were perceived to be more successful at detecting intrusions, they were not perceived to have more secure systems or less vulnerable to attacks by external parties. Finally, we found that white hat hackers were more likely to be hired when they hacked for intrinsic reasons, and reformed hackers were more likely to be hired when they hacked for extrinsic reasons. We contribute to the systems security literature by providing empirical evidence to help firms understand the importance of systems

Table 2
Results of Propositions

Panel A: Proposition 1 (Corporate security policy)

Dependent Variable	Corporate Security Policy	Mean	p-value
Vulnerability to attacks by internal parties	Yes	3.92	0.287
	No	4.24	
Vulnerability to attacks by external parties	Yes	2.48	0.051
	No	2.90	
Detection of intrusions	Yes	4.33	0.025
	No	3.59	
Security of systems	Yes	4.89	0.016
	No	4.28	
Importance of security	Yes	5.88	0.000
	No	4.74	

*70% indicated that their firms had a corporate security policy and 30% reported that their firms did not have a corporate security policy. One participant did not indicate whether her firm had a corporate security policy.

Panel B: Proposition 2a (Internal systems security audit)

Dependent Variable	Mean	F	p-value
Detection of intrusions	4.08	3.75	0.004
Security of systems	4.68	3.95	0.003
Vulnerability to attacks by internal parties	3.99	10.96	0.000

Panel C: Proposition 2b (External systems security audit)

Dependent Variable	Mean	F	p-value
Detection of intrusions	4.08	2.46	0.044
Security of systems	4.68	1.81	0.126
Vulnerability to attacks by external parties	2.61	1.96	0.100

Panel D: Proposition 3a (Intrinsic reasons for hacking)

Dependent Variable	Mean	t	p-value
Possibility of hiring white hat hackers	2.92	8.003	0.005

Panel E: Proposition 3b (Extrinsic reasons for hacking)

Dependent Variable	Mean	t	p-value
Possibility of hiring reformed hackers	1.88	2.900	0.091

*The dependent variables were based on a 7-point Likert scale with 1=not at all and 7=to a great extent.

systems security. We also provide insight into whether a person's reasons for hacking would have an impact on a firm's willingness in hiring her. Our findings offer guidance to firms facing a dilemma on whether they should hire hackers. Firms might consider hiring white hat or truly reformed hackers.

Suggestions for Future Research

The paucity of research on the behaviors of hackers might explain why the tremendous amount of resources committed to contain the problems caused by hacking has resulted in somewhat little success. Future research could examine the behaviors of hackers and compare the results with the findings of our study[14]. We found that corporate security policies did not have an impact on perceived vulnerability of firms to attacks by internal parties. This

[14] We conducted this research and found the results interesting.

finding can be explained by the fact that internal parties may be in a better position (than external parties) to overwrite or sabotage the corporate security policy put in place by their firms. Future work can provide additional insight on this issue. About 70% of our participants indicated that their firms had a corporate security policy; 59% indicated that their firms performed an internal security audit of their systems; and 29% reported that their firms hired independent contractors to review the security of their systems. Future research can help explain why firms are reluctant to increase spending on internal or external security audits of their systems. Finally, corporate security policies can be in the form of a simple informal discussion, scribbles on a piece of paper, or a well-conceived plan (www.intrusion.com). Researchers can investigate whether similar results are obtained in situations where different types of corporate security policies (e.g., formal or informal, simple or comprehensive, etc.) are implemented.

The authors wish to thank the University of Massachusetts at Boston for funding their research study.

References

1. "Advisory/Axent security expert available to discuss hiring hackers; modern day pirates or robin hoods?" (2000, August 14). Business/technology editors. *Business Wire*, 2190.
2. AMR Research: "Sarbanes-Oxley compliance spending will exceed $5 billion in 2004". (2004, January). *DM Review*.
3. Anthes, G. H. (1995, November 6). "Security plans lag computer crime rate". *Computerworld*.
4. Benson, C., Jablon, A. V., Kaplan, P. J., & Rosenthal, M. E. (1997). "Computer crimes". *American Criminal Law Review*, 34(2), 409-443.
5. Bennett, M. (2002, April 12). "Can you trust an ethical hacker?" *IT Week*. http://www.vnunet.com/
6. Callaway, E. (1996, December 23). "Breach of security". *PC Week*.
7. Campbell, D. S. (2002). "Focus on cyber fraud: The Internet has added another dimension to internal auditors' battle against fraud. Those who understand the implications of this treat can help secure the organization against online deception". *Internal Auditor*, 59(1), 28-32.
8. Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (Forthcoming). "The economic cost of publicly announced information security breaches: Empirical evidence from the stock market". *Journal of Computer Security*.
9. Cushing, K. (2001). "Would you turn to the dark side?" *Computer Weekly*.
10. e-Commerce Times. (2000). http://www.ecommercetimes.com/perl/story/4677.html.
11. Gordon, L. A., & Loeb, M. P. (2002). "Return on information security investments: Myths vs. realities". *Strategic Finance*, 26-31.
12. Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (Forthcoming). "Information security expenditures and real options: A wait-and-see approach". *Computer Security Journal*.
13. Graham, J. R., & Harvey, C. R. (2001). "The theory and practice of corporate finance: Evidence from the field". *Journal of Financial Economics*, (May/June), 187-243.
14. "Hackett Group survey reveals that nearly half of all companies ignore IT in critical elements of Sarbanes-Oxley compliance efforts". (2003, December). *DM Review*.
15. Hayes, F. (2002, December 23). "Losers & winners". *Computerworld*.
16. Hodge, F., Martin, R. D., & Pratt, J. "Qualified accounting changes and investor assessments of financial performance and representational faithfulness". Working paper.
17. Hoffman, T. (2002, December 2). "Healing touch of a one-company view". *Computerworld*.
18. Hopper, D. I. (2001, March 9). "Credit card hacker warning issued". *Associated Press*.
19. Imhoff, C. (2004, January). "Intelligent solutions: The year of compliance, Part 1". *DM Review*.
20. Johnson, M. (2002, December 2). "Cyber who cares? IT should"! *Computerworld*.
21. Locke, A. D., & Hartley, B. V. (2001, May). "Security as a process". *DM Review*. http://www.dmreview.com.
22. "Maximizing the value of network intrusion detection". (2001). http://www.intrusion.com.
23. Mulhull, T. (1999). "Where have all the hackers gone? Part 3: Motivation and deterrence". *Computers & Security*, 16, 291-297.
24. Nelson, M. W., Elliott, J. A., & Tarpley, R. L. (2002). "Evidence from auditors about managers' and auditors' earnings-management decisions". *The Accounting Review*, 77, 175-202.

25. Nevins, S. C. (2003, January). "Database security: Protecting sensitive and critical information". *DM Review*.
26. Packer, R. (2001). "Protecting the network". *Network Security*.
27. Richardson, R. (2003). "8th Annual Computer Security Institute/Federal Bureau of Investigation Computer Crime and Security Survey". Computer Security Institute.
28. Romney, M. B., & Steinbart, P. J. (2003). *Accounting Information Systems*. Prentice Hall: New Jersey.
29. Savage, M. (2003, April 21). "RSA conference spurs debate: Hacker hiring, security standards examined". *Computer Reseller News*.
30. Songini, M. L. (2002, December 2). "Tight budgets put more pressure on IT". *Computerworld*.
31. Thomas, D. (2002). *Hacker Culture*. University of Minnesota Press.
32. Thurman, M. (2001, February 26). "I hired a hacker: A security manager's confession". *Computerworld*.
33. Trahan, E., & Gitman, L. (1995). "Bridging the theory-practice gap in corporate finance: A survey of chief financial officers". *Quarterly Review of Economics & Finance*, (Spring), 73-87.
34. Verton, D. (2002, November 4). "Hacking syndicates threaten banking". *Computerworld*.
35. Wallace, B. (2001, March 9). "European hackers plunder U.S. firms, FBI says 40 victims in 20 states were hit". *San Francisco Chronicle*.
36. Weinstein, B. (2002, June 11). "Should you hire an ex-hacker?" http://www.builder.com.
37. "You need a corporate security policy". (1998, June). *e-Business Advisor*, 16(6), S6.http://www2.cio.com/analyst/report260.html.