MIS Review Vol. 18, No. 2, March (2013), pp. 81-96

The Impact of Strategic IT Partnerships on IT Security

Jason K. Deane[1], Terry R. Rakes[1], Loren Paul Rees[1], Wade H. Baker[2]
[1]*Department of Business Information Technology, Pamplin College of Business, Virginia Tech*
[2]*Director of Risk Intelligence, Verizon Business Security Solutions*

ABSTRACT: *Partnering is a common business practice which takes advantage of outside expertise and allows companies to focus efforts on their core competencies. A key component of partner coordination is information sharing. Whether a partner is a traditional partner such as a supply vendor, where the firms use information technology (IT) as a facilitator for information sharing, or an IT partner to which an organization outsources certain IT functions, IT allows partners to open information borders to each other. While beneficial in many ways, this sharing also creates security vulnerabilities which should not be ignored. In this study, we examine forensic accounts of numerous past security incidents in an effort to learn more about the impact of partner relationships on security risk, and to suggest factors which may be indicators of increased risk.*

KEYWORDS: *IT Security, IT Risk, Strategic Partnerships, IT Fraud.*

1. Introduction

In the modern global economy, reduced vertical integration and a heavy reliance on strategic corporate partnerships has become the norm (Flynn, Huo & Zhao, 2010). Organizations have increased their reliance on the outsourcing of non-core activities choosing alternatively to focus their energy and resources on their core competencies (Russell & Taylor, 2011). The economies of scale afforded by these relationships, regardless of whether the partnership is based on the delivery of direct or indirect goods or services, often motivate organizations to move away from traditional contract-driven supplier agreements and instead to move to a heavier dependence on more strategic partnerships. In doing so, companies are choosing to reduce their number of business partners in an effort to develop and grow a small number of very highly integrated relationships in lieu of maintaining a larger number of loosely integrated ones (Flynn et al.; Schliephake, Stevens & Clay, 2009).

To realize the full potential of these relationships, companies are routinely turning to advancements in technology to increase the level of transparency, openly sharing information electronically with their business partners (Du, Lai, Cheung & Cui, 2012). Within supply chains, information asymmetry between companies and their partners is one of the biggest causes of the "bullwhip effect" where upstream suppliers continually

overshoot and undershoot demand because of time lags in information. Information sharing of customer demand with strategic supply partners has greatly reduced this bullwhip effect (Fiala, 2005). In the customer service area, shared knowledge between IT and customer service units is a key capability that affects customer service performance (Ray, Muhanna & Barney, 2005). These customer service units are often partners to which we outsource customer service responsibilities. Within the tourism industry, IT has provided the support that improves a company's communications with their partners and consumers (Buhalis & Law, 2008). In virtually every area of business, IT has enhanced the ability for information sharing and information transparency with partners.

This increased transparency and sharing of information improves the accuracy and timeliness of information availability, allowing organizations to more efficiently and effectively manage all aspects of the creation and delivery of their products and services. However, often these partners are actual providers of IT services (such as point of sale services) as opposed to (for example) part or service partners in a supply chain who need to communicate. While both of these types of partnerships are vital to competitive viability in an information-driven economy, the security risks associated with information sharing, particular when the information path is privileged and automated, should not be ignored.

Data Breaches through a partner or by a partner are part of a larger, serious problem facing companies. In 2013, Verizon Business will report in their Data Breach Investigations Report that this year's dataset represents the largest they have ever covered in any single year, spanning 40,000+ reported security incidents, 588 confirmed data breaches, and approximately 44 million compromised records (that they were able to quantify). Over the entire nine-year range of Verizon's Data Breach Investigations Reports, the cumulative tally now exceeds 2,500 breaches and 1.2 billion compromised records. As this study underscores, IT security breaches, regardless of their source or nature, can be very costly and damaging to an organization's reputation and long term competitiveness. As a result, enhanced IT security is a key focus of organizations worldwide. Companies are devoting substantial resources in an attempt to secure their IT infrastructure and informational resources. Because security management is a very specialized area, many companies are turning to Managed Security Services (MSS) providers. According to Basking Ridge's report (2010), the global market for MSS providers is expected to grow by approximately 18.5% a year and to reach $14.7 billion annually by 2016. A more recent study by Ferrara (2012) put the growth estimate in the MSS provider global market at between 30% and 40% per year. MSS providers are increasingly being viewed as essential strategic partners in the quest for secure business.

Because of the variety of methods attackers use to try to infiltrate and disrupt

corporate IT infrastructures, corporate IT specialists and MSS providers have been forced to develop a wide array of actions to block these intrusions or to mitigate the damaging effects of an intrusion. One of the biggest challenges facing organizations in attempting to develop effective practices to protect their assets is predicting from where the attacks are likely to come. Most organizations focus the majority of their efforts and resources on defending against external threats. These are threats from entities that are unrelated professionally with the organization. In addition, many also work hard to defend against attacks from disloyal employees that are internal to the organization. While efforts and mechanisms to combat internal threats and external threats which originate from unknown sources are well-documented, little attention seems to have been given to the vulnerabilities created by IT relationships between partners or IT outsourcing as described earlier. We believe that many organizations are overlooking a key risk by not examining their partner relationships more closely and viewing every partner as a potential vulnerability.

We highlight through analysis of an extensive forensic dataset just how risky IT partner relationships may be. We are not proposing that organizations should avoid such relationships, but instead argue that this source of increased security risk should not be ignored, and should be a key component in security planning. In addition, we are hopeful that our analysis will help organizations understand how these relationships are commonly exploited, which technology solutions are most vulnerable, and which defense mechanisms are most effective at identifying the attacks. In doing so, we hope to help managers improve their information technology strategies as they relate to partnership development and to protecting their extremely sensitive information assets.

The remainder of this manuscript is structured as follows. In Section 2, we describe the forensic data set used in our analysis. In Section 3, we report on tests on this data which indicate that breaches through a partner are potentially more damaging than other sources of attack. In Section 4, we outline several risk attributes which could help to understand the role of IT partners in breaches and their associated risk. In Section 5, we provide several conclusions and managerial insights.

2. The data set

As the foundation of this study, we analyze a forensic data set collected by Verizon Business and the United States Secret Service (USSS) from 2007 to 2009 (Verizon Business, 2010). Verizon Business is one of many MSS providers, including AT&T, CSC, Dell SecureWorks, HP, IBM, Symantec, Trustwave, Wipro, and others. Because of its client base, Verizon is considered to be a tier 1 vendor of security services (Ferrara, 2012).

Because of their services in risk and compliance solutions, data loss and prevention, and identity management solutions, many of the world's largest businesses and governments, including 96 percent of the Fortune 1,000 and thousands of government agencies and educational institutions, rely on their services (Basking Ridge, 2010). It is client self-reporting that serves as the mechanism for collecting the data in this data set. The USSS is involved as a partner because of the legal reporting requirements for certain types of organizations or certain types of attacks. The combination of data from these two sources provides a very rich snapshot of the nature of past attacks. All of the data are sanitized so that there is no identification of any company or party to any of the incidents.

This data set consists of detailed data collected by each of these organizations as part of their investigations of 368 organizational IT security breaches over this time period. After a reported incident, Verizon and the USSS analyze the evidence and record the objective data points. Of 368 reported attacks, 108 involved a partner with an average of 713,000 records being compromised in these breaches. The median number of records compromised in these 108 attacks was also quite high. On the surface, the data supports the view that the situations that resulted in the greatest loss in terms of the median number of records compromised were breaches that involved a partner as part of the attack. In the next section, we will test specific hypotheses related to this view. Based on these findings, we will argue that it would be very beneficial for organizations to look more closely at attributes of their partner relationships so that they better understand this key source of risk.

3. Analysis of partner risk

Losses from security breaches can take many forms (damaged or lost equipment, comprised client information, tarnished company reputation, etc.). However, one of the most tangible and often-used measures of data breach severity is the number of compromised records. This is likely due to the presence of studies that have objectively quantified the financial loss associated with compromised records. In their 2013 study of 277 organizations in nine different countries, Symantec calculated the average cost to an organization per compromised record to be $136 (Symantec, 2013). In the US, the figure was somewhat higher at $188 per compromised record. Thus, breaches involving a substantial number of compromised records can justifiably be categorized as financially severe security events. As mentioned earlier, one of the data items collected in the Verizon/USSS data set is the number of records compromised (for those breaches where records were the target of the attack, which were the vast majority).

In our study, we focus on the median number of records compromised during an

attack as opposed to the mean. The mean is significantly affected by outliers, and there are certainly a few breaches where an extraordinarily large number of records were compromised (the largest recorded breach was over 150M records). Because of several very large breaches, the mean number of records affected across all types of breaches was over 2.5M, while the median was only 40K records. Because of these outliers, we feel that the median is a much more accurate measure of typical severity.

When analysts think of the typical source of threats, they generally look to sources external to the organization (hackers, former employees, identity thieves, etc.) who have no business relationship with the company. External sources might be considered a benchmark for threat profiles. Thus, our first goal is to compare the median number of records compromised for breaches that originated solely with a partner to those that originated externally. There were 170 security incidents which originated purely from a partner or an external source. The external source group had a median of 35,003 records, while the partner only group had a median of 212,500 records. While the partner group has a much higher median, in order to determine whether there is a statistically significant difference between the two groups, we propose the following hypotheses:

H1: The median number of records compromised during partner source only attacks is not significantly different from the median number of records compromised during external source attacks.

H1a: The median number of records compromised during partner source only attacks is significantly greater than the median number of records compromised during external source attacks.

To test this hypothesis, we employ the non-parametric Mann-Whitney U Test (also referred to as the Wilcoxon Rank Sum Test). Provided that the observations are drawn from continuous distributions and that the hypothesis involves only a shift in location (i.e. that the variances are equal), the Mann-Whitney U Test (MWU Test) can be interpreted as a test of difference in medians (Lehmann, 2006). To address the issue of equal variances, we ran the Brown-Forsythe Test (Brown and Forsythe, 1974) which is considered to be the most robust test for equality of variances when the underlying distributions are skewed (non-normal). For the Brown-Forsythe Test (BF Test) for these two groups, we obtain an f-value of 2.699 with 167 degrees of freedom. This results in a p-value of .1023, which indicates that there is not sufficient evidence (at a significance level of .05) that the variances are different. Thus, the underlying assumptions of the MWU Test are confirmed.

To conduct the MWU Test, we first rank order all of the observations (number of compromised records) for both groups as one set, and then sum the ranks for each group. For group one, we calculate the test statistic

$$U_1 = R_1 - n_1(n_1+1)/2$$

where n_1 is the sample size for the first group and R_1 is the sum of ranks. We then calculate U_2 in a similar manner and use the smaller of U_1 and U_2 when consulting significance tables. For our data groups, U = 2,168 and the one-tailed p-value is .0315. Thus, at the .05 significance level, there is evidence in the study to reject H1 and conclude that the partner incidents had a higher median number of compromised records.

As a further comparison, we compare the partner only group to all other breaches (external, internal, and all combinations of sources). There were 289 breaches in this combined data set, with the partner only group having a median of 252,000 compromised records, and the combination of all other groups having a median of 30,001. Thus, we propose the hypotheses:

H2: The median number of records compromised during partner source only attacks is not significantly different from the median number of records compromised during attacks from all other sources or combinations of sources.

H2a: The median number of records compromised during partner source only attacks is significantly greater than the median number of records compromised during attacks from all other sources or combinations of sources.

For these hypotheses, the BF Test yields an f-value of 1.1857 with 184 degrees of freedom, for a p-value of .2776. At the .05 significance level, this indicates that there is not conclusive evidence that the variances are unequal, and that we are justified in using the MWU Test. The MWU Test yields a test statistic value of U = 4,068.5 and a one-tailed p-value of .0117. At the .05 significance level, we once again reject the null hypothesis in favor of the alternate, which suggests that the partner only attacks seem to be more severe.

While there is no direct evidence in the data to suggest why the partner source attacks are more severe, one can speculate. Given the trusted status afforded most partners and the IT access which is routinely granted, when attacks do come through this vector they are likely to be severe and may go undetected for some period of time. In the next section, we discuss several risk attributes that emerge from the data, and attempt to explain why they are particularly problematic when dealing with partners.

4. Partner risk attributes

Based on the potential severity of IT partner-based security breaches, it is obvious that organizations could benefit by understanding more about these attacks. We hope to

help organizations by analyzing many of the key attributes and trends of these breaches. To that end, we define seven attributes of IT partner-related incidents as follows:

(1) the type of IT partner relationship

(2) the manner in which IT partners caused or contributed to an incident

(3) the victim's industry

(4) whether an attack was targeted or opportunistic

(5) the type of malware, hacking, or intrusion that was involved

(6) the vector(s) or pathway(s) exploited by this hack/intrusion to breach the perimeter and access internal resources

(7) the mode of discovery of the breach

Except for attributes (1) and (2), the remainders of these attributes are not unique to partner-related incidents and will also apply to incidents which originate internally or from external non-partner sources. However, we are primarily interested in the degree to which partner-related incidents exhibit these attributes. We believe that examining these issues will help us shed some light on the IT security risks associated with the development of strategic partnerships and further our understanding of the attribute characteristics that were present when information assets were breached as a result of a partnership, and thereby suggest ways to mitigate these risks. For the analysis in this section, we will include all breaches in which a partner played a roll (partner only, external and a partner, internal and a partner, and the combination of all three sources). In the data set, there were 108 observations that fit this profile.

4.1 Type of IT partner relationship

The type of IT partner relationship represented by breach incidents was quite varied. As we look at the list of relationships, keep in mind that we are focusing on the part that IT automation and communication or IT outsourcing plays in the relationship as opposed to the actual business relationship. Therefore, the types of relationships are described in terms of the IT services that are provided or outsourced to form or support the relationship. For example, to share information with a supply vendor, we may contract with a third party, or use third party software, to create and host a web portal for real-time sharing. In this sense, both the vendor and the IT support company are strategic partners in this relationship, but we are only interested in the vulnerability created by the IT component of the relationship. If we contract with a partner for cloud services, we may actually be outsourcing several of these IT functions in a single relationship with one partner. In our data set, the types of IT relationships included (1) remote IT

management/support, (2) hosting provider, (3) security services/consulting, (4) data storage/archiving, (5) merchant processing services, (6) onsite IT management support, (7) telecommunications provider, and (8) software developer/vendor. While each of these was represented, remote IT management/support was the dominant type of IT relationship in the 108 breaches, representing 87 of the breaches (hosting provider was the next most frequent with 9). Because remote IT management/support is a broad category, it may be beneficial to look at a more precise measure by examining the assets that were actually involved in these breaches. In these 87 breaches, point-of-sale (POS) terminals and POS servers were mentioned 95 times as assets that were attacked, with POS servers being the more frequent target because of the larger set of financial data available to the hacker. Note that the number of assets attacked can be larger than the number of attacks because one attack can target many different assets. While other assets are mentioned, such as database servers, web app servers, VPN servers, file servers, self-service kiosks, etc., none was involved nearly as often as POS terminals and servers.

POS is a particularly fertile target for thieves because "cash, cards, inventory and customer data intersect at the point of sale" (Fitzgerald, 2008). POS attacks can be especially severe if hacking of a POS server goes undetected for a long period, putting numerous financial records at risk. Advancements in technology have helped, such as giving POS personal identification number (PIN) pads their own media access control (MAC) address so that they can be disabled immediately when a breach is detected (Fitzgerald). However, as the breach data shows, a POS relationship where a third party is trusted to collect payments remains a very risky type of IT partner outsource.

4.2 Partner's role in the incident

Partners can play various roles in an incident from being unintentional conduits for malicious entry to being an active player in the breach. In this data set, in 71 of the 108 breaches (66%) which involved an IT partner, another agent acted via the partner's assets or access path to gain entry. It is not surprising that such a large number of breaches involved this partner role. The privileges and access afforded to partners serves as an ideal target for the malicious intruder. This large number of incidents underscores the importance of security assurance, to the point of only contracting with partners who have undergone and passed a stringent security audit. MSS providers often perform these security audits, and their stamp of approval is at least some assurance that the IT partner is doing everything possible to provide secure information transfer. It is important for a firm to extend its security beyond its own walls.

What is surprising is that 29 of the reported incidents (27%) involved a partner who acted deliberately and maliciously. The key fact to remember here is that your partner is only as reliable as their least reliable employee. One disgruntled employee, or one

employee tempted to commit larceny, located at a strategic IT partner can be the catalyst for a major security incident. Once again, security audits and making sure the partner follows best practices in regard to preventing insider abuse are the best defenses.

The final 8 breaches (7%) were the result of a partner who acted inappropriately or unintentionally without malice. These are cases where an unintentional action or omission on the part of the partner created vulnerability.

4.3 Victim industry

It is clear from Figure 1 that the hospitality, retail, and financial sectors are prime targets for partner attacks. This should not be surprising given our earlier findings about the vulnerability of POS operations. The hospitality and retail industries are major users of POS technology, and the financial industry, such as payment processing and card clearing, is also a victim when information is stolen from POS servers or other financial databases. Financial institutions often assume the liability for at least a portion of losses when credit cards or account information is stolen. This also points out that there can be multiple victims in an incident, often including both the victimized organization and its partners. In a POS server attack, the retail organization is a victim, perhaps suffering loss of reputation and time and cost associated with client notification and restitution. The customer is a victim because their personal information is stolen and exposed. And, the financial institution that participates in the POS operation may be a victim if they are liable for the losses in lieu of the customer. Once again, the relationship created by partnering with other groups who provide POS services or rely on those services creates numerous avenues of vulnerability.

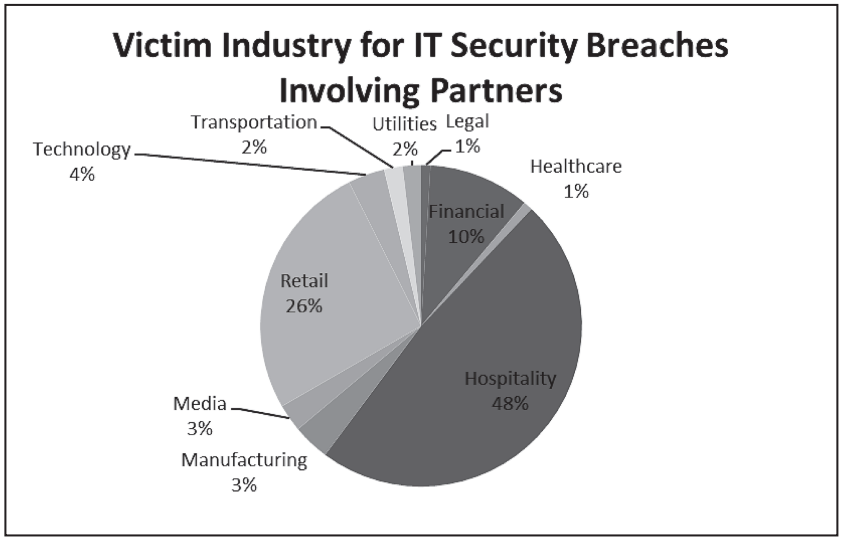

Figure 1 Victim Industry

Figure 1 also seems to indicate that no industry is immune from potential partnering risk. Industries such as transportation, media, utilities, and legal may not immediately come to mind when we think of possible targets for attacks, but they still are at risk. Obviously, thieves are going to most often target the industries where they can steal the most money or records. However, any industry can be an attractive target if it is easy to attack and highly vulnerable. In the next section, we talk about attacks where the victim(s) is a target of opportunity.

4.4 Targeted or opportunistic

In this forensic compilation, victims were asked if the incidents were targeted or opportunistic. Surprisingly, only 10 of the 108 victim organizations identified the attacks as being targeted. This directly implies that 91% of the incidents were not pre-meditated and instead resulted from the attacker simply stumbling upon an opportunity/vulnerability. Even if a firm is vigilant about its security policies, a window of opportunity may open at the partner's location, giving access to assets.

Obviously, windows of opportunity can open and close constantly. A password scribbled on a piece of paper can carelessly be left by a computer or server today, but can be thrown out with tomorrow's trash. Someone looking over your shoulder can see a PIN and decide to utilize it for an attack. Access to a secure server room can be compromised when a door is inadvertently left unlocked or unattended. In all of the cases, it is unlikely someone planned the incident ahead of time; rather, individuals were able to gain entry or access because of a poor security policy, or poor enforcement of a security policy. Also, when a hacker sees the opportunity to act on a temporary vulnerability, the attack is often technologically unsophisticated but can nonetheless be very damaging. The implication for organizations is that many of these breaches could probably have been avoided if the organization in question afforded a little more attention to the policies, strategies, and enforcement related to IT security. When a partner has access to your assets, one of the best ways to assure that they do not create windows of opportunity is to periodically ask for an IT audit of their policies and enforcement procedures.

4.5 Type of attack

In an effort to better understand the nature of attacks, we examined the types of intrusions that occurred when a partner was involved. As is shown in Figure 2, many types of attacks occurred, including brute force dictionary attacks, cross-site scripting, SQL injection and back door exploitation. However, the vast majority of the attacks involved login credentials. This is consistent with our earlier findings where many attacks were against servers (such as POS servers or web-hosting servers). If hackers are able to gain login access to a server, most if not all of the assets on that server are at risk. 35%

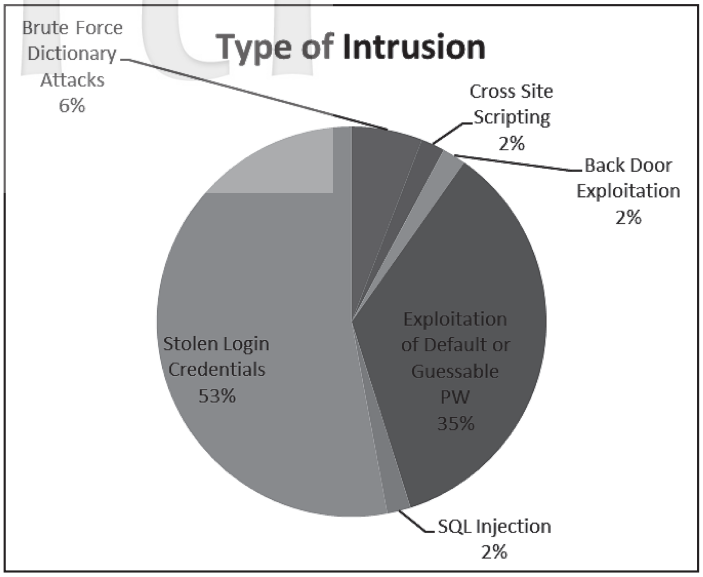

Figure 2 Type of Intrusion

of the attacks occurred via the exploitation of guessable or default passwords and 53% using stolen login credentials. This is disturbing in that it highlights situations that for the most part should be easily avoidable. While there may be situations where criminals go to extreme measures to illegally acquire a user's login credentials, using guessable or default passwords is extremely sloppy and represents a very poor enforcement of security policy. In those situations where credentials are stolen or compromised, these could often be avoided with better policies as well, limiting opportunities for the hackers. It is to a firm's advantage to make sure that its employees and partners' employees are diligent in their development and adherence to login and password protection, and that policies are updated and examined frequently. The forensic data should serve as a wakeup call to those organizations that have ignored the importance of these policies. In a private communication, Verizon Business (2013) reports to us that this has become even more important in the last few years. They suggest that if you want to gain access to *Secure Corporation X*, why not just target X's weak partner and nab its administrative credentials to X's systems?

4.6 Intrusion vector or pathway

In an effort to learn more about attack modalities, the victims were asked to identify the vector or pathway that was exploited in the data breach. The results of the responses to this question are presented in Figure 3. Out of 108 partner-related security breaches, only four types of vectors or pathways were identified. Four percent of the criminals gained access through a backdoor or control panel, 6% through a web application, 7% via remote

access services (such as VPN or dial-up access) and 83% through remote desktop/admin services (such as *pcAnywhere* or *LogMeIn*). Clearly, enabling remote desktop/admin services creates a major conduit that hackers can exploit. While it is important to secure all of the possible attack pathways, disabling as many remote desktop programs as possible (and having a strong security policy against their use which carries penalties for violation) would go a long way toward preventing unauthorized access. Obviously, for firms that must have a remote admin services provider, this creates a dilemma as one must provide a way for the provider to remote in.

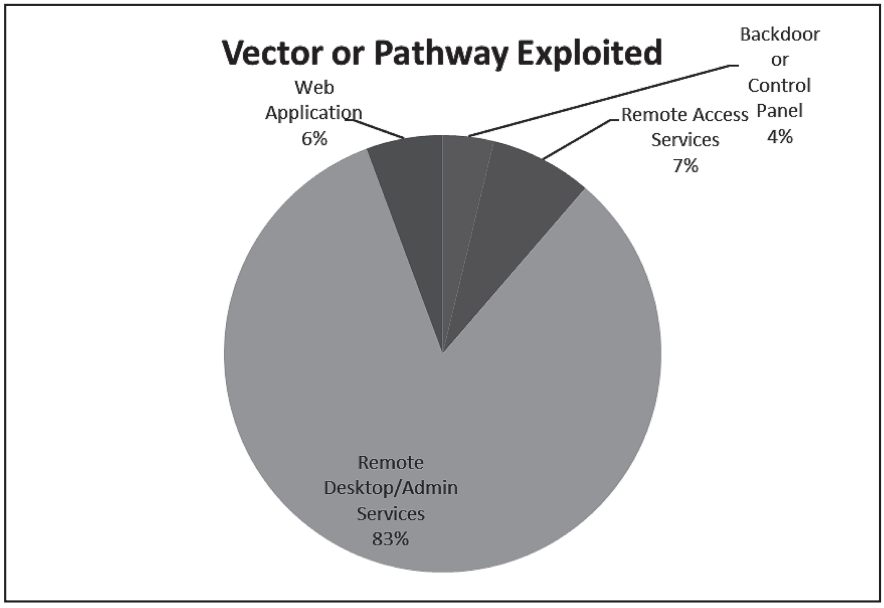

Figure 3 Attack Vectors and Pathways

4.7 Breach detection

Finally, victim organizations were asked to identify how they detected the breach. The results of this question are presented in Figure 4. A few breaches were detected through such means as unusual system behavior, identification by law enforcement, reports from affected customers, detection during internal audits, etc. However, the vast majority were detected through the utilization of third party fraud detection systems/ software. This highlights the importance of, and provides support for, organizational investment in these products. Given that resources are often scarce and that expenditure on fraud detection software may often be overlooked, these data serve as motivation for organizations to make this investment.

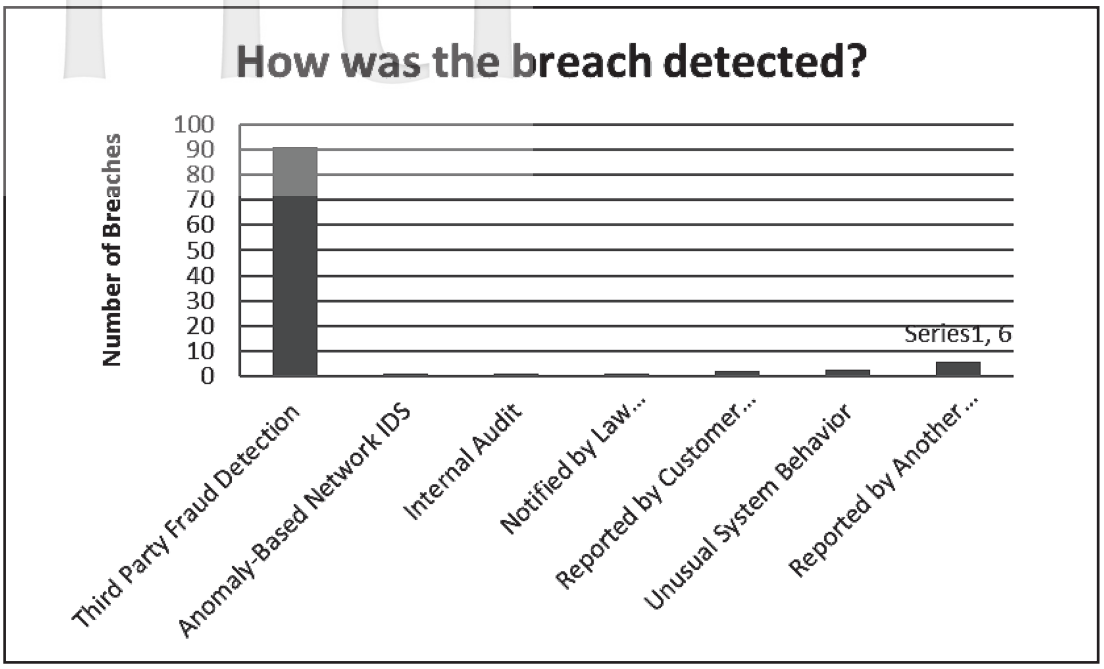

Figure 4 Breach Detection

5. Conclusions and managerial implications

Organizations are increasingly partnering with other organizations and/or outsourcing both products and services in order to streamline operations and focus on core competencies. To make these arrangements work, IT becomes an essential part of these partner relationships. However, IT systems also provide additional, and often fertile, attack pathways for hackers. In this study, we have examined a powerful forensic data set which reveals many of the attributes of past partner-related attacks. From our analysis, several conclusions emerge. (1) In terms of severity of an attack measured by the median number of records compromised (which is often used as a surrogate for financial loss), attacks which originated with a partner were more severe than either external or internal attacks. (2) While there are many types of IT partnership arrangements which have resulted in data breaches, remote IT management/services seems to be the most frequent. Within the IT services domain, point-of-sale seems to be an area that has been highly vulnerable. (3) While a significant number of attacks involved a partner or partner's employee that acted deliberately and illegally, the majority of attacks involved the exploitation of a partner's access pathway or assets without the partner's knowledge. (4) Based on the frequency of occurrence, no industry seems to be immune to partner attacks. However, organizations

that are in the hospitality, retail and financial industries seem to be especially at risk. (5) The majority of partner attacks in this data set were opportunistic. Organizations must be constantly vigilant to prevent windows of opportunity for hackers. (6) Stolen login credentials are a major opportunity for hackers, and represent one of the most frequently reported types of attack. Guessable or default passwords should always be avoided, and strong security policies in regard to passwords should be enforced, both for one's own employees and those of partners. (7) Organizations should consider very carefully their utilization of remote desktop/administration services such as *pcAnywhere* and *LogMeIn*, given that these applications were the attack vector exploited in more than 80% of the partner-related security breaches. (8) Breach detection can occur in many ways, but most often is aided by third-party fraud detection software. It is imperative that this type of software be used by both the company and by its partners to quickly close off any vulnerability.

Given that partner relationships are a necessary and powerful strategic arrangement, but one carrying additional risk, we recommend that organizations should enact the following. First, develop a strong internal IT security policy outlining the methods and procedures for selecting partners who present the least risk. Next, continuously asses each partner's risk posture by demanding periodic IT security audits by independent third party examiners, for example. These audits will assure that access pathways are secure, login credentials are protected, etc. Finally, invest in fraud detection software so that when inevitable breaches do occur, they will be quickly detected so that damage can be mitigated. While many of these findings appear to be commonsense and reinforce what others have advised in the literature, we hope that seeing forensic proof will provide companies with the motivation to strengthen their security postures in the specific manners outlined. This vigilance will allow companies to enjoy the benefits afforded by strategic partner relationships.

References

Basking Ridge, N.J. (2010), 'Frost & Sullivan Ranks Verizon Business as a top provider of global managed security services', *Verizon*, available at http://www.verizonbusiness.com/about/news/pr-25607-en-Frost+%26+Sullivan+Ranks+Verizon+Business+as+a+Top+Provider+of+Global+Managed+Security+Services.xml (accessed 4 February 2013).

Brown, M.B. and Forsythe, A.B. (1974), 'Robust tests for equality of variances', *Journal of the American Statistical Association*, Vol. 69, No. 346, pp. 364-367.

Buhalis, D. and Law, R. (2008), 'Progress in information technology and tourism management: 20 years on and 10 years after the Internet -- the state of eTourism research', *Tourism*

Management, Vol. 29, No. 4, pp. 609-623.

Du, T.C., Lai, V.S., Cheung, W. and Cui, X. (2012), 'Willingness to share information in a supply chain: a partnership-data-process perspective', *Information & Management*, Vol. 49, No. 2, pp. 89-98.

Ferrara, E. (2012), 'The Forrester wave™: Managed security services: North America, Q1 2012', *Trustwave*, available at https://www.trustwave.com/ .../The_Forrester_Wave_MSS_2012.pdf (accessed 4 February 2013).

Fiala, P. (2005), 'Information sharing in supply chains', *Omega*, Vol. 33, No. 5, pp. 419-423.

Fitzgerald, M. (2008), 'Security at the point of sale', *CSO Online*, available at http://www.csoonline.com/article/458175/security-at-the-point-of-sale (accessed 7 February 2013).

Flynn, B.B., Huo, B. and Zhao, X. (2010), 'The impact of supply chain integration on performance: a contingency and configuration approach', *Journal of Operations Management*, Vol. 28, No. 1, pp. 58-71.

Lehmann, E.L. (2006), *Nonparametrics: Statistical Methods Based on Ranks*, Springer, New York, NY.

Ray, G., Muhanna, W.A. and Barney, J.B. (2005), 'Information technology and the performance of the customer service process: a resource-based analysis', *MIS Quarterly*, Vol. 29, No. 4, pp. 625-652.

Russell, R.S. and Taylor, B.W. (2011), *Operations Management: Creating Value Along the Supply Chain*, John Wiley & Sons, New York, NY.

Schliephake, K., Stevens, G. and Clay, S. (2009), 'Making resources work more efficiently -- the importance of supply chain partnerships', *Journal of Cleaner Production*, Vol. 17, No. 14, pp. 1257-1263.

Symantec (2013), '2013 Cost of data breach study: United States', *Ponemon Institute*, available at http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-us-report-2013.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach (accessed 22 July 2013).

Verizon Business (2010), '2010 Data Breach Investigations Report', *Verizon*, available at http://www.verizonenterprise.com/resources/executivesummaries/es_2010-data-breach-report_en_xg.pdf?r=88 (accessed 9 February 2013).

Verizon Business (2013), '2013 Data Breach Investigations Report'. Conveyed via private conversation.

About the authors

Jason K. Deane is Associate Professor of Business Information Technology in the Pamplin College of Business at Virginia Tech. He received a Ph.D. in Decision and Information Sciences from the University of Florida, and an M.B.A. and B.S. in Business Administration from Virginia Tech. His current research interests are in the areas of artificial intelligence, computer-aided decision support systems, information system security, large scale optimization and information retrieval. He has published in such journals as *Decision Support Systems*, *Annals of Operations Research*, *Information Technology and Management*, *International Journal of Physical Distribution and Logistics Management*, *Operations Management Research*, and others.

Terry R. Rakes is William and Alix Houchens Professor of Information Technology at Virginia Tech. He received the Ph.D. in Management Science, M.B.A., and B.S.I.E. from Virginia Tech. His research interests are in analytics and big data analysis, text and data mining, geographic information systems, disaster planning and logistics, information security, and the application of decision support and artificial intelligence methodologies to problems in information systems. He has published in *Management Science*, *Decision Sciences*, *Decision Support Systems*, *Annals of Operations Research*, *OMEGA*, *European Journal of OR*, *Operations Research Letters*, *Information and Management*, *Journal of Information Science*, and others.

Loren Paul Rees is Andersen Professor of Business Information Technology. He received the Ph.D. in Industrial and Systems Engineering, B.E.E. from Georgia Tech, and M.S.E.E. from the Polytechnic Institute of Brooklyn. Dr. Rees' current research focuses on managerial issues in information technology security; on nonparametric simulation optimization; and on the application of wireless broadband capabilities to rural and/or developing areas. He has published in *Naval Research Logistics*, *IIE Transactions*, *Decision Sciences*, *Transportation Research*, *Journal of American Medical Informatics Association*, *Journal of the Operational Research Society*, *Computers and Operations Research*, *Communications of the ACM*, *Decision Support Systems*, and others.

Wade H. Baker is Managing Principal of RISK Intelligence for Verizon Business, where he oversees the collection, analysis, and distribution of all internal and external data relevant to better understanding and managing information risk. Baker has a master's degree in information technology from the University of Southern Mississippi and is in the final phase of obtaining his Ph.D. in Business Information Technology at Virginia Tech. He has published in *Communications of the ACM*, *IEEE Security & Privacy*, the *International Journal of Electronic Marketing and Retailing*, and others.