Integration of Information Systems and Cybersecurity Countermeasures: An Exposure to Risk Perspective

Richard Baskerville
Georgia State University and Curtin University

Frantz Rowe
Université de Nantes and SKEMA Business School

François-Charles Wolff
Université de Nantes

Acknowledgments

We thank the Editorial team at *Data Base*, Jean-Loup Richet for his feedback, as well as participants at ICIS and LEMNA (Université de Nantes) where the paper was subsequently presented. This research was funded by Région des Pays de la Loire and sponsored by competitive Poles EMC2 and Novalog as part of the OLASI program.

Abstract

This paper investigates the relationship between Information Systems (IS) integration and the use of cybersecurity countermeasures using an adapted exposure to risk perspective which considers both the probability of a risk through vulnerability points theory and the impact of the risk if it occurs. Based on an econometric analysis of a survey sample of 9,721 French firms, the study finds that higher degrees of system integration entail higher degrees of cybersecurity usage. Whereas previously it was thought that systems integration reduces the number of vulnerabilities and thus the need for cybersecurity countermeasures, we find that the more the system is integrated, the greater the use of self-protective cybersecurity countermeasures. We theorize that this finding comes from the elimination of many uncontrollable vulnerabilities and the presence of fewer, but controllable, vulnerability points. This finding holds both for internal and external integration but is stronger in the latter case. Moreover, results show that internal dynamism is positively correlated with cybersecurity countermeasures. Our reasoning applies to cybersecurity in terms of self-protective security measures but not necessarily to risk-transfer security measures.

Keywords: Cybersecurity Countermeasures; Internal Integration; External Integration; Internal Dynamism; Exposure to Risk; French Firms.

Introduction

It is a longstanding information systems principle that increasing systems integration, such as through the adoption of an enterprise system and the associated supply chain integration, quite naturally increases the control that management exercises over their information, and thereby their organization (Besson & Rowe, 2001). It is easy to conclude that this control principle also implies that increasing systems integration naturally increases the security of these systems, in the sense that fewer additional security countermeasures are needed for integrated systems.[1] The research we report below shows that such a conclusion is not justified. On the contrary, greater integration is associated with a larger investment in self-protecting security controls and countermeasures.

Since the first large empirical studies of American firms, we know that firms do too little to protect themselves against computer abuse (Straub, 1990). This might have changed with the advent of the Internet in the 1990s and the growth of broadband in the 2000s. While myriad computer abuses are reported daily and cybersecurity countermeasures have been developed (including such technologies as

anti-virus software, firewalls, access-control authentication/encryption, and secured servers), we still know very little about whether and how firms choose to protect themselves and the organizational contingencies that drive such protection decisions. Organizations often conceal their security profiles because such profiles might disclose their vulnerabilities. As a result, it is difficult to determine empirically how organizations are equipped and how their cybersecurity equipment might relate to their IS architecture and their external environment.

Whereas cybersecurity seems to be a growing concern, the integration of Information Systems (IS) has always been an enduring quest of IS literature (Tanriverdi et al., 2010). In particular, growth of enterprise systems has been a major phenomenon in IS over the last 30 years (van Everdingen et al., 2000). The aim of this paper is to investigate the potential relationship between the degree of IS integration and the acquisition of cybersecurity countermeasure technologies.

Such a relationship is not obvious as IS cybersecurity countermeasures may come with software or equipment vendor pressure (Lee & Larsen, 2009), regardless of the firm's IS integration level. Integration without cybersecurity or with fewer cybersecurity investments may no longer be the option it might have been in an ideal world where capability threats or malicious intentions do not grow with the wider perimeter for action afforded by highly integrated systems. If an integrated system is compromised, then it may have a greater impact—affecting all integrated functions both internal and external—than a non-integrated system which would be confined to just one system. This relationship between IS integration and security countermeasures might also be contingent upon a variety of organizational characteristics such as firm size or industry (Straub, 1990; Galbreth & Shor, 2010). The current context and in particular environmental dynamism can also affect fundamental aspects of vulnerability (Keats & Hitt, 1988).

Specifically, we develop and test a set of hypotheses that are derived from an exposure to risk perspective concerning this relationship. Risk exposure regards the probability of an undesirable outcome compounded by the level of the loss if it occurs (Barki et al., 1993; Aubert et al., 1998). Integration of information systems, particularly in the case of enterprise systems, ought to *reduce* this risk exposure. Yet our data confirm a seeming contradiction, i.e. that such integration coincides with an *increased* level of "spend" for cybersecurity technology.

We theorize that the increase in cybersecurity spend is actually an unexpected product of the reduction of risk exposure that accompanies system integration. System integration brings IT risk exposures down from levels so extreme that these have been unmanageable. The exposure falls to manageable levels that enable organizations to identify affordable and appropriate cybersecurity technologies. We will draw on the theory of vulnerability points (Suleiman & Svetinovic, 2013) to elaborate how these seemingly contradictory phenomena unfold and support it with an empirical analysis of a substantial set of survey data.

We position our contribution in the emerging literature on the organizational perspective on information security (Ransbotham & Mitra, 2009). Functional integration of information systems is often driven by the adoption of packaged Enterprise Resource Planning (ERP) systems (Olhager and Seldin, 2003). ERP systems often address many cybersecurity requirements inherently (Wada et al., 2008). Information security experts advocate building in systems security from the ground up, rather than bolting it on after system development, in order to avoid making security a secondary task that conflicts with system integration (McDermott & Fox, 1999; Yee, 2004).

Because organizations often conceal their security profiles, the IS integration security relationship has largely been anchored in opinion, argument, and theory, but with rather limited empirical evidence to support it. As with other aspects of information security, field data is difficult to obtain. Available data on cybersecurity behaviors is often obtained through qualitative case studies and face-to-face interviews (Kotulic & Clark, 2004), or expressed as the written opinion of experts in the practical press.

In this paper, we study the relationship between IS integration and cybersecurity countermeasures with more objective empirical data than past studies. The assumptions are formulated as a theory of exposure to risk as an IS becomes more integrated and generates a different composition of risk exposure and, in turn, different cybersecurity countermeasures. Our empirical analysis relies on a unique data set of nearly 10,000 French firms surveyed in 2006 about various aspects of their economic activity as well as their cybersecurity countermeasures. The remainder of our presentation is organized as follows. In the next section, we elaborate the model and present our hypotheses. Following this elaboration, we present the research methodology and results. The discussion and conclusion follow.

Theoretical Framework and Hypotheses

IS Integration, Internal and External

IS integration has been an enduring quest in IS, both practically and conceptually (Tanriverdi et al., 2010). The literature generally distinguishes between

technical IS integration and cognitive IS integration (Beretta, 2002; Markus, 2001; Marciniak et al., 2014). In this paper, IS integration refers only to the former, which we define as the capability to directly process data through connectivity and a single logical database with a unique human intervention so that the modified data is available for other applications using the same database. This availability is important because IS integration does not only mean connectivity, but also business interdependence (Venkatraman, 1994). In this view, IS integration serves to increase automation and reduce user load and errors. Typically, with IS integration, data reentry can be dramatically reduced if not totally eliminated (Venkatraman, 1994). This does not imply that the number of data entry points is systematically reduced (even though integration is often accompanied by optimization of such data entry functions), but it does mean that IS integration is often an occasion for business process reengineering and rationalization of entry points. As a result, the frequency of data reentry and the number of data entry points generally diminish with IS integration.

The above reasoning holds for both internal and external IS integration. Internal integration (integration across systems within the same organization) arises when a company replaces different systems equipping different functions with an ERP system that covers all the corresponding functions (Bidan et al., 2012). External integration (integration across systems between different organizations) arises when companies collaborate to replace inefficient data exchanges (such as paper-based orders and invoices) with a data interchange system (Kim et al., 2006; Rajaguru & Matanda, 2013; Lairet et al., 2016). Processing data varies from data consulting to updating (modifying and even deleting data). The processing outcomes differ depending on the types of systems involved. In some systems, partners can only consult (e.g. extranet) while in others partners can transfer data for treatment (e.g. Electronic Data Interchange).

IS Vulnerability and Vulnerability Points Theory

An information system vulnerability is the intersection of three conditions: (1) system susceptibility, such as a design or implementation flaw; (2) threat accessibility, such as system access points or services; (3) threat capability, such as an opponent with the knowledge and resources to discover, access, and exploit a flaw (Brumley et al., 2008; Hughes & Cybenko, 2014). Threat capability can be reinforced by the attractiveness of the target considering its data and its functionalities. Cybersecurity can remove vulnerabilities by eliminating one or more of these three conditions. A *vulnerability point* specifies a location in a system or process where a vulnerability can be triggered or actuated (Nappa et al., 2015). Vulnerability points coincide with one or more cybersecurity requirements (Suleiman & Svetinovic, 2013). These requirements address one or more of the vulnerability conditions. Therefore a vulnerability point is known to be a *controllable* vulnerability with a calculable risk level (Suleiman & Svetinovic, 2013). The analysis of vulnerability points, sometimes called data exposure control points, has been an aspect of information security methodologies for decades (Fisher, 1984).

Vulnerability points are notable at junctions where data cross over boundaries into, out of, and between systems. Such junctions create additional work to translate the outputs of one system to match the input requirements of another system (Leifer, 1989). This "entropy" can sometimes be more ad hoc and create additional vulnerabilities. For example, Fisher's (1984) vulnerability points included those points in the overall system where data makes transitions: data collection points, data conversion points, data communication points, data storage points, and data disposition points. Oladimeji et al. (2011) provide an example of a vulnerability point analysis of a health interchange system.

Below, we theorize that systems integration reduces the number of uncontrollable vulnerabilities and produces instead a smaller number of (controllable) vulnerability points. A more integrated system has fewer and less diverse boundary crossings than a less integrated system. Such systems tend to define a standard set of user interfaces and object access protocols. These sets replace a larger number of ad hoc interfaces in less integrated systems. Accordingly, these smaller sets can be more rigorously developed, more carefully tested and more frequently audited for such security vulnerabilities as buffer overflows and SQL injection.

Figure 1 is a simple representation of two systems. In the left part of the diagram, a less integrated system (System *x*) operates as multiple independent-but-connected subsystems (subsystem 1 and subsystem 2). Likely vulnerabilities are identified whenever subsystem boundaries are crossed. On the left side of the diagram we see many potential vulnerabilities (V1-V18) typical of non-integrated systems (System *x*). These are typical because of bespoke interfaces subject to high degrees of costly software maintenance. These may be quite risky because these must be accessible from outside the two subsystems in order to communicate information in and out of the systems. They might well be regarded as uncontrolled vulnerabilities because they are numerous and both difficult and costly to identify and correct. In the right part of the diagram, an integrated system (System *y*)

might duplicate the functionality of System *x*. There are fewer vulnerabilities because many boundary crossings have been incorporated internally, and there are fewer, more standardized interfaces at the remaining boundary crossings. With fewer, standardized vulnerabilities, it becomes more feasible to specify affordable countermeasures for each vulnerability. Because these become controllable vulnerabilities, we denote them as vulnerability points (VP1-VP4).

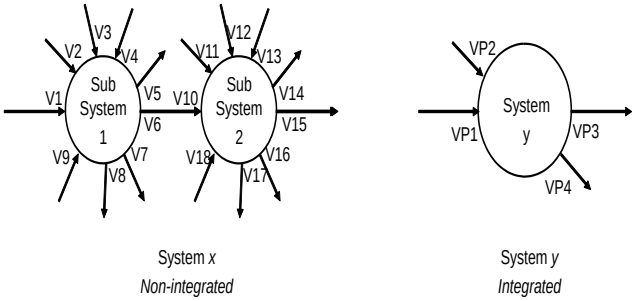

Figure 1. Vulnerabilities in a Less Integrated System (System *x*) Versus Vulnerability Points in a More Integrated System (System *y*)

Reducing the number of vulnerabilities affects the overall number of conditions for vulnerabilities. Fewer vulnerability points can mean standardized accessibility and fewer opportunities for accessible flaws. Why then should we expect the cost of the technology to deliver cybersecurity countermeasures to rise following a transition from System *x* to System *y*? The answer lies in the conversion of vulnerabilities to vulnerability points.

Managing Cybersecurity Risk Exposures

Like other forms of risk management, cybersecurity risks align with the common risk treatment framework (Jones & Ashenden, 2005). This framework maps various kinds of risk treatments (such as market insurance, countermeasures and controls) into categories suitable for different degrees of threat likelihood and threat impact as shown in Figure 2. Self-protection, the common treatment for high likelihood and low impact threats, includes most technology-based safeguards such as virus control software and firewalls. In contrast, lower likelihood and higher impact are treated with risk transfer techniques such as business interruption insurance whereby the risk is transferred to the insurance company. Lower likelihood and lower impact risks are treated with self-insurance, meaning that risk is accepted by the organization and losses are recovered using corporate reserves. Risks that are of higher likelihood *and* higher impact are treated by avoidance strategies, such as abandoning such operations or business lines.

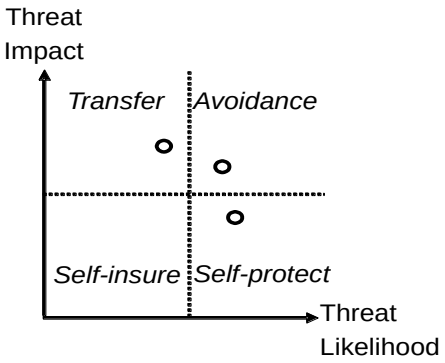

Figure 2. Risk Management Framework (adapted from Jones & Ashenden, 2005)

While the framework can be used with different kinds of scales, it also provides a conceptual model of the aims and approaches of risk management. The risk management literature regards treatment indications that are related to likelihood and impact of threats (Boehm, 1989; Aubert et al., 2005; Huang & Nan, 2008). We will use the term *risk exposure* to reflect a vulnerability's threat likelihood and impact comparatively to others (Barki et al., 1993; Aubert et al., 1998). Risk exposure is essentially the conceptual distance of a vulnerability from the zero-risk origin. Thus the three circles in Figure 2 conceptually represent three different vulnerabilities (e.g., an unpatched system in the presence of good maintenance (unlikely but impactful), a buffer overflow in bespoke software (likely and impactful), or a cleartext transaction (likely but not impactful when controlled by encryption)). While these are equally exposed to risk in the sense they are equally distant from the origin, their ideal treatment might be different (e.g., insure against business interruption, reorganize to eliminate bespoke systems, encrypt the system).

Figure 3 represents the conceptual cybersecurity situation when a non-integrated system (*x*) graduates to an integrated system (*y*). It illustrates how the risk management situation (Figure 2) changes relative to a change in system integration (Figure 1). The circles (Figure 3, System *x*) represent a large population of uncontrollable vulnerabilities (i.e., numerous and costly, as above). The closed dots (Figure 3, System *y*) represent a smaller population of controllable vulnerability points (i.e., fewer and identifiable) arising from the reduced boundary crossing. Many vulnerabilities disappear (as described above, and remembered only as grey circles), some change the nature of their exposure to risk and become vulnerability points, and perhaps a small number of new vulnerability points will appear.

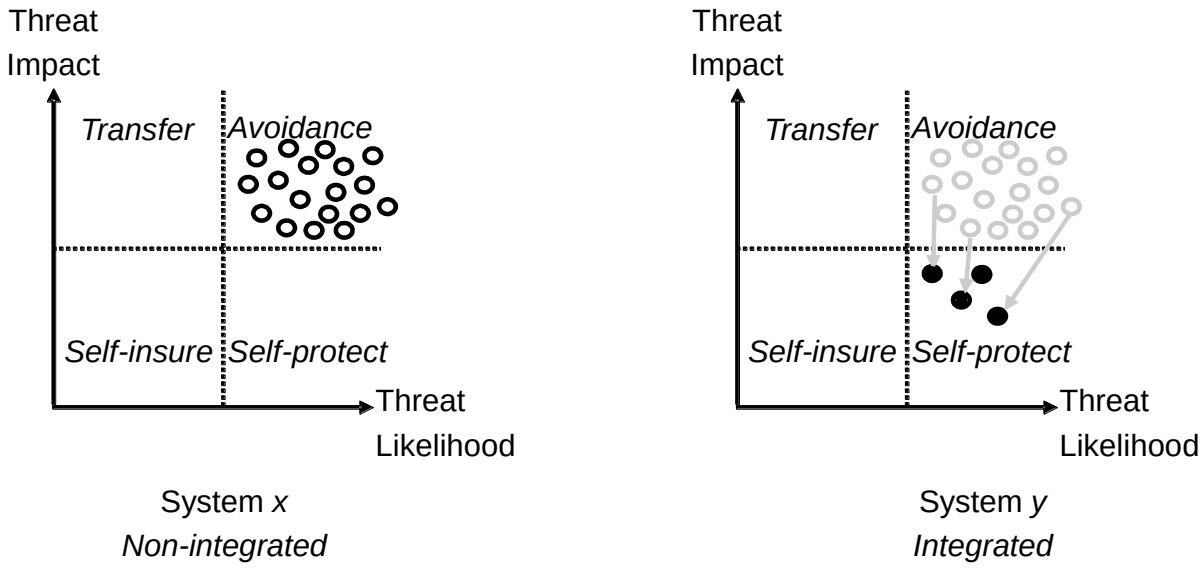

Figure 3. Effect of Integration on the Risk Management Situation

We theorize that such a conceptual transition from a situation with System *x* to a situation with System *y* would predict that system integration would be accompanied by greater spend on technology for cybersecurity protective countermeasures. Integration eliminates many uncorrectable and prohibitively grave vulnerabilities, but creates instead a feasible number of vulnerability points that are correctable with self-protection cybersecurity technologies. In addition, many firms do not want to fully integrate their IS architecture internally (Bidan et al., 2012), some precisely because they do not believe that such countermeasures can be effective (Bidan & Rowe, 2004). So, if firms move to higher levels of IT integration, we can assume that they have identified appropriate cybersecurity countermeasures. Responsible risk management would command acquisition of such technologies along with the integration. Our central hypothesis is:

> Hypothesis 1 (H1): The greater the IS is integrated, the more the firm will invest in technology for self-protection cybersecurity countermeasures in the firm's information system.

We have mentioned two different examples of system integration. One is the adoption of an enterprise system, such as an ERP (internal integration). The other is the integration of a supply chain, such as the adoption of data interchange (external integration). While it would not be unusual for these two forms of integration to coincide, the effects illustrated in Figure 3 are likely to be more extreme in the case of external integration because the system boundary crossings are reduced to very few indeed (i.e., often only one or two standard interfaces). However, the boundary crossings in this situation not only cross system boundaries but also organizational boundaries. Such vulnerability points involve higher risk exposure because uncertainty is higher. Cross organizational vulnerabilities will always involve actors and system controls that are external to the organization of interest and unknown. For the same reasons, the exposure conditions (threat capability) are also unknown. For example, such interfaces have to be rigorously protected from unauthorized outsiders (e.g., hackers). This protection is made less certain because some outsiders, such as workers at partner organizations, are *somewhat* insiders.

> Hypothesis 2 (H2): The positive relationship between integration and cybersecurity spend (H1) will be stronger with external IS integration than with internal IS integration.

Self-protection operates on the grounds of past experience with threats that enable estimates of future threats occurrences based on a continuation of similar events. It is a form of evidence-based cybersecurity in which evidence enables prediction and estimation of the likelihood and impact of a reoccurring event (Bahill & Smith, 2009). Typical risk analysis involves quantification of probabilities and losses based on history (Baskerville, 1991) or such other evidence as shaped by human beliefs (Sun et al., 2006). Self-protection actions such as the acquisition of cybersecurity technologies are taken immediately, and certainly prior to the next predicted event. In a volatile environment, we can expect threat capabilities to change frequently. These external changes mean that cybersecurity technologies must be frequently reconfigured or reacquired.

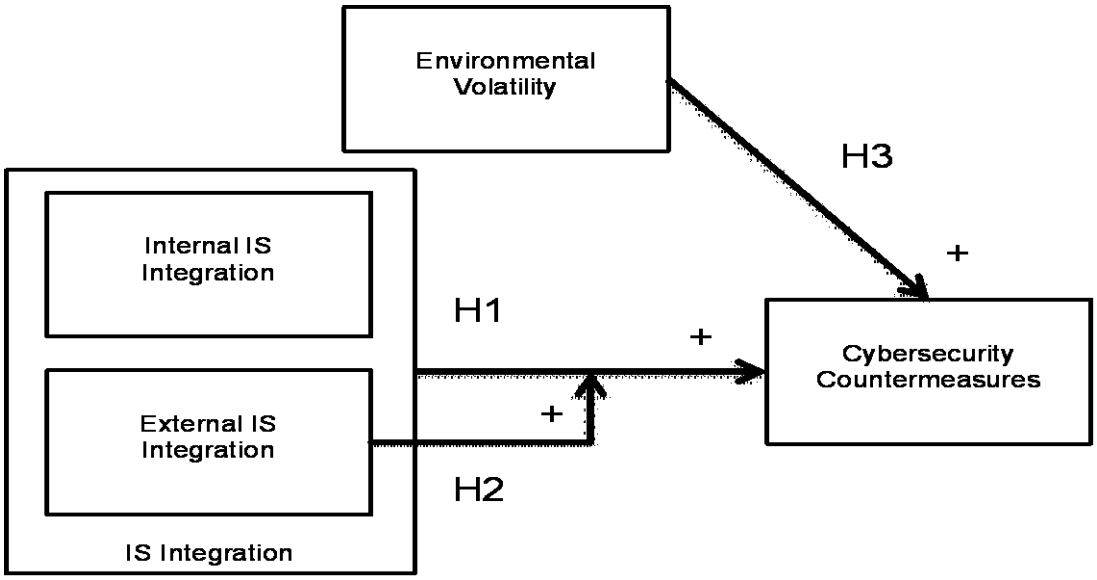

Figure 4. Research Model

However, volatile environments also affect internal dynamism so that like any other business process volatile environments drive self-protection to be more dynamic.

In organization theory and IS, the literature characterizes environmental uncertainty in terms of dynamism, munificence (or growth), and complexity of the environment, and such "dynamism refers to the volatility and unpredictability of the changes that a business unit has to deal with" (Keats & Hitt, 1988; Xue et al., 2011, p. 391). More dynamic systems change more frequently and unpredictably. This volatility means that, in addition to the external threat capability, the internal system susceptibility and threat accessibility are liable to more frequent change. As a result, environmental volatility can affect all three fundamental aspects of vulnerability. Conceptually, this means vulnerability point requirements must be more elaborate to address all three aspects of vulnerability. These elaborated vulnerability point requirements are more likely to demand multiple cybersecurity technologies for each point. We would expect to see an increase in the diversity of cybersecurity technologies required to satisfy the updated and effective vulnerability point requirements.

> Hypothesis 3 (H3): In highly volatile environments, firms will use a greater diversity of self-protection cybersecurity countermeasures than in less volatile environments.

Our hypotheses are represented diagrammatically in Figure 4.

Data and description of variables

To study the relationship between cybersecurity countermeasures and IS integration within firms, we rely on a large survey conducted by the French National Institute of Statistics and Economic Studies (INSEE) in 2006. The survey, called the Organizational Changes and Technologies of Information and Communication (COI-TIC) survey, aimed to focus on the extended enterprise and functional-related aspects of IS integration.

The survey was pre-tested at the national level by INSEE. One of the authors, nationally recognized as an expert in IS, participated in its design and pre-tested it with three firms. Altogether it was pre-tested with 20 firms, and the feedback was discussed by the design team. The pre-test was focused on the correct understanding of the firms and led to the rewording and elimination of certain questions or items. It also led to refining the interview guide that provided definitions given to the interviewee when they had problems understanding what was meant. INSEE sent questionnaires by regular mail to a nationally representative sample of about 17,000 firms (randomly drawn) with at least ten employees.[2] Possibility was given to call INSEE for more detailed explanations in case of difficulties. Those who sent the questionnaires knew the firms and had been trained on this questionnaire by the design team, and notably by the expert who is one of the authors. The response rate was equal to 85 percent, and 13,790 firms filled in the questionnaire, corresponding to a weighted sample of 163,099 firms of ten employees and more representative of the French economy.[3]

As our aims deal with IS integration, we decided to select the subsample of firms having the six following functions either internally managed or managed by a subcontractor or a service provider: i) marketing, ii) production, iii) finance, iv) R&D, v) human resources, and vi) logistics. This left us with an unweighted sample of 9,721 firms, the weighted size being equal to 102,615 firms. In doing so, we restrict our attention to multi-functional firms that are by definition larger on average. For instance, the proportion of firms with 500 or more employees is 16.5 percent in our sample while the corresponding proportion amounts to 13.9 percent in the original sample.

Our research aims relate this integration to the acquisition of technologies that deliver cybersecurity countermeasures. The information security literature is replete with analyses of countermeasures. Some classify these into four types: deterrence, prevention, detection, and recovery (Straub & Welke, 1998; Warkentin & Willison, 2009). Another refers to five types: access, vulnerability, feature, traffic, and audit control (Ransbotham & Mitra, 2009). The ISO/IEC guidelines organize IT security controls into 14 groups (ISO/IEC, 2013). The Payment Card Industry (PCI) standard specifies 12 requirements organized under six goals: secured systems and networks, protected data, managed vulnerabilities, controlled access, monitored networks, and maintained policy (PCI Security Standards Council, 2016).

The PCI approach is best suited to our research setting because its focus is consistent with vulnerability point theory, its scope is suitable for a very wide range of organizational types and sizes, and its requirements are among the most explicit in terms of countermeasure technologies. Requirement 1 specifies firewalls, requirement 5 specifies anti-virus software, requirements 6 and 8 specify secured servers, and requirements 4, 7, and 8 specify encryption and access authentication. The remaining requirements do not regard countermeasure technologies but rather organizational procedures and policies. We investigated the four PCI-required cybersecurity countermeasure technologies (virus protection, firewalls, secured servers, and authentication/encryption mechanisms).[4]

According to the COI-TIC survey, firms have on average a relatively high level of cybersecurity equipment. The average number of cybersecurity countermeasures is three. 40.1 percent of these firms have the four countermeasures, 30.9 percent have three, 19.4 percent have two, 7.0 percent have one and 2.6 percent have none. Anti-virus software and firewalls, either hardware or software, are found respectively in 96.3 percent and 83.2 percent of the multi-functional firms. Secured servers using access protocols such as https are also frequently used (69.7 percent). Authentication/encryption mechanisms such as digital signature, PIN code, or data encryption is adopted by around one-half of firms (49.6 percent). Overall, this pattern suggests that multi-functional firms invest in cybersecurity countermeasures but to a lesser extent in practices that may involve more time and cognitive effort. The mean number of countermeasures is relatively constant across sectors, except in construction (2.6) and finance (3.4). These differences are explained by the level of severity of data error risk and mitigation rules within these sectors.

We construct both internal and external integration indicators from a large set of questions in the COI-TIC survey (see the Appendix for details). Internal integration, which allows relevant information about business activities or transactions to be shared within the firm, depends on the use of ERP respectively for the R&D, purchase, sales, production, human resources, and accounting departments (Bidan et al., 2012), the presence of a central database respectively for R&D, sales, human resources, and accounting (De Corbière et al., 2012), and the presence of database interface tools such as EAI or SOA (Sharif & Irani, 2005). Overall, we consider 11 items for internal integration.

The measurement of external integration, i.e. how companies and business partners integrate systems at different points in a supply chain, relies on the following 12 questions that were drawn from the literature: whether the firm uses an extranet or web portal dedicated to partners (Lairet et al., 2016); whether the firm uses an EDI; whether the firm uses tracking tools; whether purchasing/sales delivery systems are coupled with either supply software, billing software, or operations software (Sharif & Irani, 2005); whether the firm receives or places orders through internet or EDI (Lairet et al., 2016); whether its largest client has its system coupled for orders and billing with that of the firm (Sharif & Irani, 2005); and whether the firm has its system coupled with its largest suppliers for orders and billing (Sharif & Irani, 2005).

A central issue consists in aggregating these various integration outcomes (respectively 11 internal outcomes and 12 external outcomes) into two synthetic indicators. Rather than relying on an ad hoc procedure like equal weights for the various components of the synthetic indicator, we consider instead a principal component analysis to determine endogenously these weights (Jolliffe, 2002).[5] Specifically, for each component of integration, we use the first principal component as synthetic indicator since it explains by definition the largest possible amount of variation in the data. The proportion of the covariance explained by the first component was

respectively 39.0 percent for the internal index and 28.0 percent for the external index.

The mean values of our synthetic indicators are by construction set to 0, their standard deviations being equal to 2.07 (internal) and 1.83 (external). Integration (either internal or external) is higher within firms characterized by larger values of the corresponding score. De Corbière et al. (2012) show the coherence of such internal and external indicators. For instance, the internal score of integration is much higher for firms with a large number of functions computerized and for those using ERPs, while the external score is much higher when orders are placed or received by computer networks or when there is supply chain management software.

The COI-TIC survey sheds light on some aspects of both the external and internal components of environmental dynamism (Robles, 2011), and measured related changes that have affected the firm between 2003 and the date of the survey. In the questionnaire, the external component of environmental dynamism focuses more on the unpredictability of the changes, while the internal component focuses more on the volatility of the changes which are more under the control of the firm. In line with our theoretical framework, we will only focus on internal dynamism when operationalizing environmental volatility.

Our internal dynamism indicator is based on questions related to organization changes since 2003. Each firm surveyed indicates whether it has experienced i) a financial restructuring (merger, acquisition, sale, buy-out), ii) organizational restructuring, iii) relocation of part of the production (offshoring), iv) location of new sites abroad (without relocation). On average, 29 percent of firms have experienced a financial restructuring, 42.2 percent an organizational restructuring, 6.6 percent some offshoring and 10.8 percent an extension of business activities abroad. We also know the strategic importance of new products for the firm and consider that there is a strategic need for novelty when survey answers mentioned either a strong or very strong importance. This concerns 59.4 percent of firms in our sample. Finally, we sum up the five dummies to obtain our indicator of internal dynamism (see the Appendix).

Results

The relationship between IS integration and cybersecurity countermeasures is at the heart of our contribution. We begin by examining the correlation between the values of the normalized indicators of internal and external integration and the number of cybersecurity countermeasures.[6]

According to the COI-TIC survey, the number of cybersecurity countermeasures is related to integration of IS. Firms characterized by a high degree of either internal or external IS integration are on average well equipped with IS security countermeasures. Compared to a firm without any cybersecurity countermeasures, the score of internal integration is four times higher for a firm using the four cybersecurity countermeasures (0.404 instead of 0.100). The same calculation gives a ratio of 3.6 for external integration (0.423 instead of 0.118). The coefficient of correlation between internal integration and cybersecurity countermeasures (0.356) is slightly higher than what is found for external integration (0.346). However, a statistical test comparing correlations (Steiger, 1980; 2005) shows that these two coefficients are not different at the conventional level with a test statistic equal to 1.106 and a p-value of 0.134 for the null assumption of equal correlations.

At a more detailed level, Figure 5 shows that the positive correlation between integration and cybersecurity countermeasures is observed for each specific countermeasure. For each tool, we find very similar coefficients of correlation for internal and external integration.[7] The proportion of firms having secured servers is equal to 81.6 percent for firms highly internally integrated (defined as the fourth quartile of internal integration), but it is only 48.6 percent for the lowest quartile. Among the more internally integrated firms, the equipment rate is 17.0 percentage points higher for firewall, 15.8 points for secured server, and 17.8 points for authentication/encryption mechanisms. The situation is very similar for firms characterized by a high level of external integration. The equipment rate is respectively 14.9 percentage points higher for firewall, 18.9 points for secured server and 24.8 points for authentication/encryption mechanisms. Albeit descriptive, these results obtained for the various countermeasures support a positive relationship between integration and cybersecurity as emphasized in H1.

Next, we take into account the role played by observable firm characteristics. Cybersecurity countermeasures are expected to depend not only on contingency factors such as environmental dynamism but also on control variables such as firm size, economic activity, geographic market, and belonging to a group. They may also be related to factors that are potentially relevant to a network economy, such as internet bandwidth and type of internet access (Ransbotham & Mitra, 2009). Indeed, the higher the bandwidth and the more vulnerable the internet access is perceived, the greater the likelihood that firms will implement cybersecurity countermeasures to mitigate their exposure to risk.

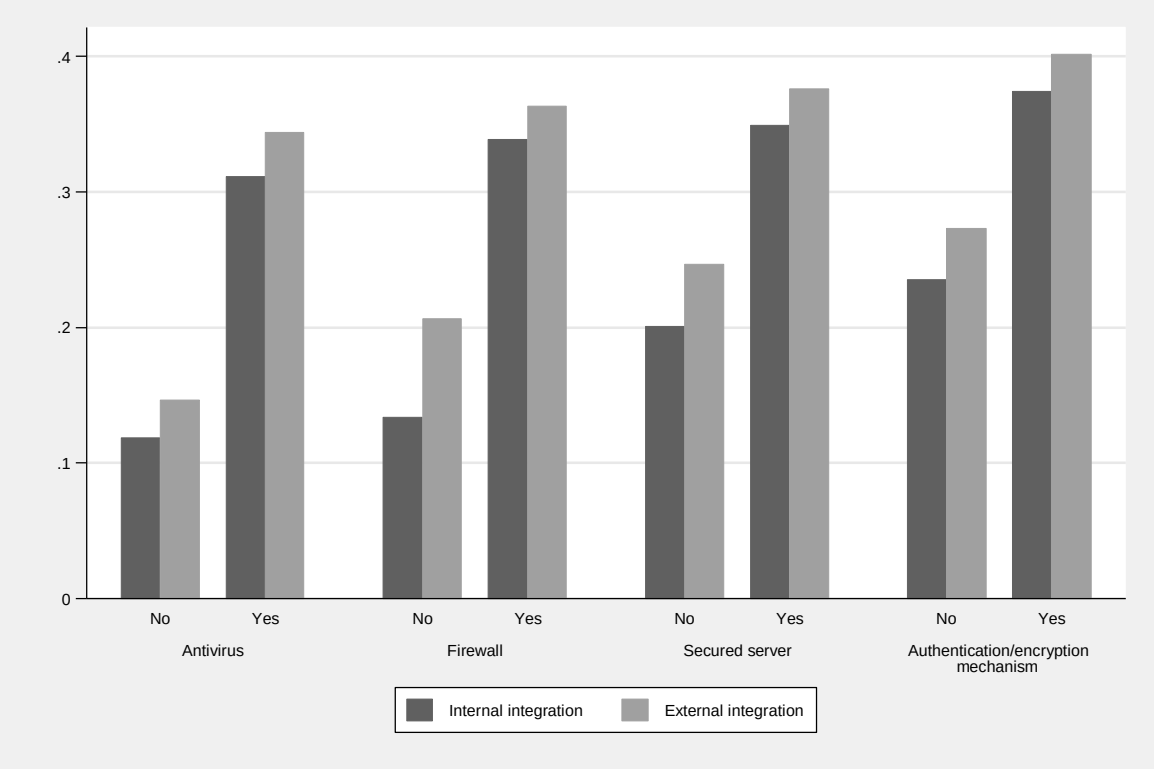

Figure 5. Average Score of External/Internal Integration, by Type of Cybersecurity Countermeasures

Source: survey COI-TIC 2006, authors' calculations.

We turn to an econometric analysis to explain the various probabilities of using each specific cybersecurity countermeasure. For the ease of the presentation, we rely on linear probability models and estimate a seemingly unrelated regression (Zellner, 1962) so that each coefficient may be interpreted as a marginal effect.[8] We also estimate the number of cybersecurity countermeasures using an Ordinary Least Squares regression.

In a first specification (Table 1), we begin by introducing only the two indicators of internal and external integration when explaining investment in cybersecurity countermeasures. We find that the number of cybersecurity countermeasures increases with the level of integration (at the 1 percent level). This positive correlation is found for both internal and external integration, which supports H1.

Table 1. Estimates of Cybersecurity Countermeasures - Without Firm Characteristics

Variables	Number of countermeasures	Antivirus	Firewall	Secured server	Authentication /encryption mechanism
Internal integration	0.952***	0.053***	0.298***	0.293***	0.308***
External integration	0.971***	0.089***	0.206***	0.303***	0.374***
Constant	2.372***	0.918***	0.672***	0.506***	0.276***
Number of observations	9721	9721	9721	9721	9721
R^2	0.164	0.028	0.093	0.083	0.091

Source: survey COI-TIC 2006, authors' calculations.

*Note: estimates from an OLS regression for the number of countermeasures and from a SUR model for the four cybersecurity countermeasures. Significance levels are respectively 1% (***), 5% (**) and 10% (*), standard errors are not reported.

Both covariates explain 16.4 percent of variation in number of countermeasures between firms. Without control variables, we observe that the coefficient obtained for internal integration (0.952) is slightly lower than that found for external integration (0.971), but the difference is not statistically significant (with a p-value of 0.798). At a more detailed level, the likelihood of using antivirus, firewall, secured server, or authentication/encryption mechanisms is positively correlated with integration. The marginal effect associated to internal integration is higher than that for external integration for firewall, but the reverse pattern is found for antivirus and authentication/encryption mechanism.

We introduce a set of control variables in Table 2. Net of the role played by the characteristics of the firm, the number of cybersecurity countermeasures remains an increasing function of both internal and external integration, which is consistent with H1. However, we find much lower values for the integration indicators once we account for firm characteristics. This is due to the fact that the integration indicators themselves vary depending on the type of firms.

Table 2. Estimates of Cybersecurity Countermeasures - With Firm Characteristics

Variables		Number of countermeasures	Antivirus	Firewall	Secured server	Authentication/ encryption mechanism
Internal integration		0.301***	-0.006	0.119***	0.097***	0.091***
External integration		0.673***	0.066***	0.113***	0.203***	0.291***
Internal environmental dynamism		0.022**	0.000	0.005	0.007	0.010**
Industry Agro-business		-0.363***	-0.017*	-0.092***	-0.135***	-0.119***
	Consumption goods	-0.264***	-0.017**	-0.070***	-0.075***	-0.102***
	Equipment goods	-0.255***	-0.003	-0.065***	-0.107***	-0.079***
	Intermediary goods	-0.256***	-0.005	-0.063***	-0.095***	-0.093***
	Construction	-0.163***	0.014*	-0.071***	-0.066***	-0.041**
	Commerce	-0.218***	-0.032***	-0.066***	-0.052***	-0.068***
	Transportation	-0.175***	-0.023***	-0.057***	-0.058***	-0.037*
	Finance and real estate	0.202***	0.015*	0.038**	0.063***	0.086***
	Firm services	Ref	Ref	Ref	Ref	Ref
Firm Size 10-19 employees		Ref	Ref	Ref	Ref	Ref
	20-49 employees	0.134***	0.022***	0.036***	0.048***	0.027*
	50-249 employees	0.280***	0.034***	0.098***	0.094***	0.053***
	250-499 employees	0.309***	0.031***	0.115***	0.075***	0.088***
	500+ employees	0.340***	0.026***	0.098***	0.095***	0.121***
Group belonging		0.228***	0.007	0.035***	0.102***	0.084***
Network belonging		0.091***	0.005	0.003	0.051***	0.032**
Market Scope	Local/regional	Ref	Ref	Ref	Ref	Ref
	National	0.085***	0.022***	0.055***	0.017	-0.009
	European	0.033	0.019***	0.049***	0.001	-0.036**
	International (outside EU)	0.087***	0.026***	0.063***	0.015	-0.018
Internet ISDN		0.195***	0.013***	0.070***	0.056***	0.055***
connection	DSL	0.310***	0.107***	0.136***	0.067***	0.000
	Other	0.204***	0.014***	0.022***	0.076***	0.092***
	Wireless connection	0.126***	0.002	-0.002	0.035***	0.092***
Bit rate	< 144 Kbit/s	Ref	Ref	Ref	Ref	Ref
	≥ 144 Kbit/s and < 2 Mbit/s	0.364***	0.074***	0.131***	0.107***	0.051***
	≥ 2 Mbit/s	0.511***	0.071***	0.159***	0.166***	0.115***
Constant		1.548***	0.737***	0.381***	0.267***	0.163***
Number of observations		9721	9721	9721	9721	9721
R^2		0.326	0.120	0.200	0.175	0.175

Source: survey COI-TIC 2006, authors' calculations.

*Note: estimates from an OLS regression for the number of countermeasures and from a SUR model for the four cybersecurity countermeasures. Significance levels are respectively 1% (***), 5% (**) and 10% (*); standard errors are not reported.

Contrary to Table 1, we now get a coefficient for external integration which is twice as high as that found for internal integration. A Wald test gives a value of 25.65 for the corresponding statistic (with a critical probability of 0.000), meaning that H2 is supported by the data. As the integration coefficients were not different without control variables, we conclude that neglecting the role of firm characteristics to explain investment in cybersecurity countermeasures leads to misleading conclusions.

When considering the various cybersecurity countermeasures, the correlation between cybersecurity countermeasures and either internal or external integration is always positive and significant except for the coefficient of internal integration in the antivirus equation, which is not significant. Again, these results support H1. When considering each tool, we find significant differences when comparing the marginal effect of the internal and external integration scores. The incidence of external integration dominates for antivirus, secured server, and authentication/encryption mechanism, with values equal to 23.39, 8.87, and 26.97 for the corresponding Wald tests. Conversely, there is no significant difference in the effect of internal and external integration for firewall. Overall, we consider that H2 is supported.

As shown in Table 2, numerous contingency factors explain investment in cybersecurity countermeasures. The type of industry plays an important role. Taking services as the reference category, the rate of presence for each countermeasure is higher in the finance and real estate sector. As expected, larger internet passive presence requires more access and traffic control (Ransbotham & Mitra, 2009). Firm size and firm association with a group correlates positively to presence for each cybersecurity countermeasure. For firms belonging to a network, secured servers and authentication/encryption mechanisms are more frequently used. The influence of market scope on cybersecurity is less clear and remains insignificant for secured servers and authentication/encryption mechanisms (except for European). Broadband and ubiquitous connectivity are positively correlated with the various cybersecurity countermeasures. Except for antivirus, the equipment rate increases by more than 10 percentage points when the speed rate exceeds 2 Mbits.[9]

Finally, Table 2 sheds light on the correlation between internal dynamism and adoption of the various cybersecurity countermeasures. Once integration is controlled for, we find a positive association between the number of cybersecurity countermeasures and dynamism (at the 5 percent level) albeit the marginal effect is of low magnitude. However, there is no positive correlation between the specific countermeasures and internal dynamism except for authentication/encryption mechanism. This suggests that firms do not focus on one specific type of cybersecurity countermeasures when facing a volatile environment but choose instead to increase their cybersecurity by accumulating different countermeasures. The positive correlation between number of countermeasures and internal dynamism tends to support H3.

So far, we have treated the synthetic integration scores as exogenous when explaining cybersecurity decisions within firms since the scores were simply introduced as additional controls in the regressions. However, integration (either internal or external) is itself an outcome whose level will be chosen by the firm depending on its own characteristics like size or sector of activity. Given the selection process of firms deciding their own level of integration, the assumption of exogeneity is unlikely to hold.[10] This selection may potentially bias the effect of the integration scores in the various cybersecurity equations. Ideally, an instrumental variable is needed to properly take endogeneity into account. However, the French COI-TIC data does not include instruments having the ideal properties, i.e. being strongly correlated with the endogenous integration scores but having no direct influence on cybersecurity other than through integration. Therefore, we decided to account for endogeneity using a selection on observables method.

We draw on recent developments in the evaluation literature and consider a matching estimator to take into account the influence of pre-treatment control variables (Heckman et al., 1998). Matching is a nonparametric technique that allows taking into account differences in pre-treatment characteristics in observational data. Matching will prune observations from the data so that after matching the empirical distributions of the selected covariates in the treated and control groups are more similar (Austin, 2011). While the literature has essentially focused on the case of binary treatment (i.e. the observation unit is either treated or not treated), in many observational studies, the treatment is not binary and takes instead a continuum of values.

In our setting, both the internal and external integration indicators are considered as continuous treatments whose values range between 0 and 1. We thus rely on the extension of the propensity-score method proposed by Hirano and Imbens (2004) which consists in estimating a dose-response function. The dose-response curve corresponds to a graph which will relate the magnitude of integration to the response in terms of cybersecurity. Implementation requires the estimation of a generalized propensity score which is defined as the conditional density of the treatment (integration in our setting) given a set of firm

characteristics (Bia & Mattei, 2008). Conditional on those observable covariates and subject to an unconfoundedness assumption (Hirano & Imbens, 2004), the intensity of integration can be considered as random for firms belonging to the same strata of generalized propensity score.

Given that the internal and external integration indicators are not normally distributed in our sample, we turn to the flexible generalized linear model recently proposed by Guardabascio and Ventura (2014) to estimate the generalized propensity score. We include the following set of covariates to calculate this propensity score: type of industry, firm size, group belonging, network belonging, and market scope. Then, we express the conditional expectation of each cybersecurity outcome as a linear function of the treatment level (intensity of integration, either internal or external) and a quadratic function of the generalized propensity score. Finally, the estimated regression function is averaged over the score function at different levels of the treatment. We plot the estimated dose-response functions obtained respectively for internal integration and external integration in Figure 6.

Our main finding is that accounting for selection on firm observables does not affect the relationship between cybersecurity and integration. First, for the four cybersecurity countermeasures, we observe that the probability of using the various tools is an increasing function of the integration score. The slope of the integration-cybersecurity is higher for tools like secured server or authentication/encryption mechanism than for antivirus. This pattern clearly supports H1, both for internal and external integration. Second, while the dose-response functions are very similar for antivirus and firewall whatever the type of integration, we note that the slope of the dose-function is steeper for external integration than for internal integration when considering secured server and authentication/encryption mechanism as cybersecurity countermeasures, which is consistent with H2.[11]

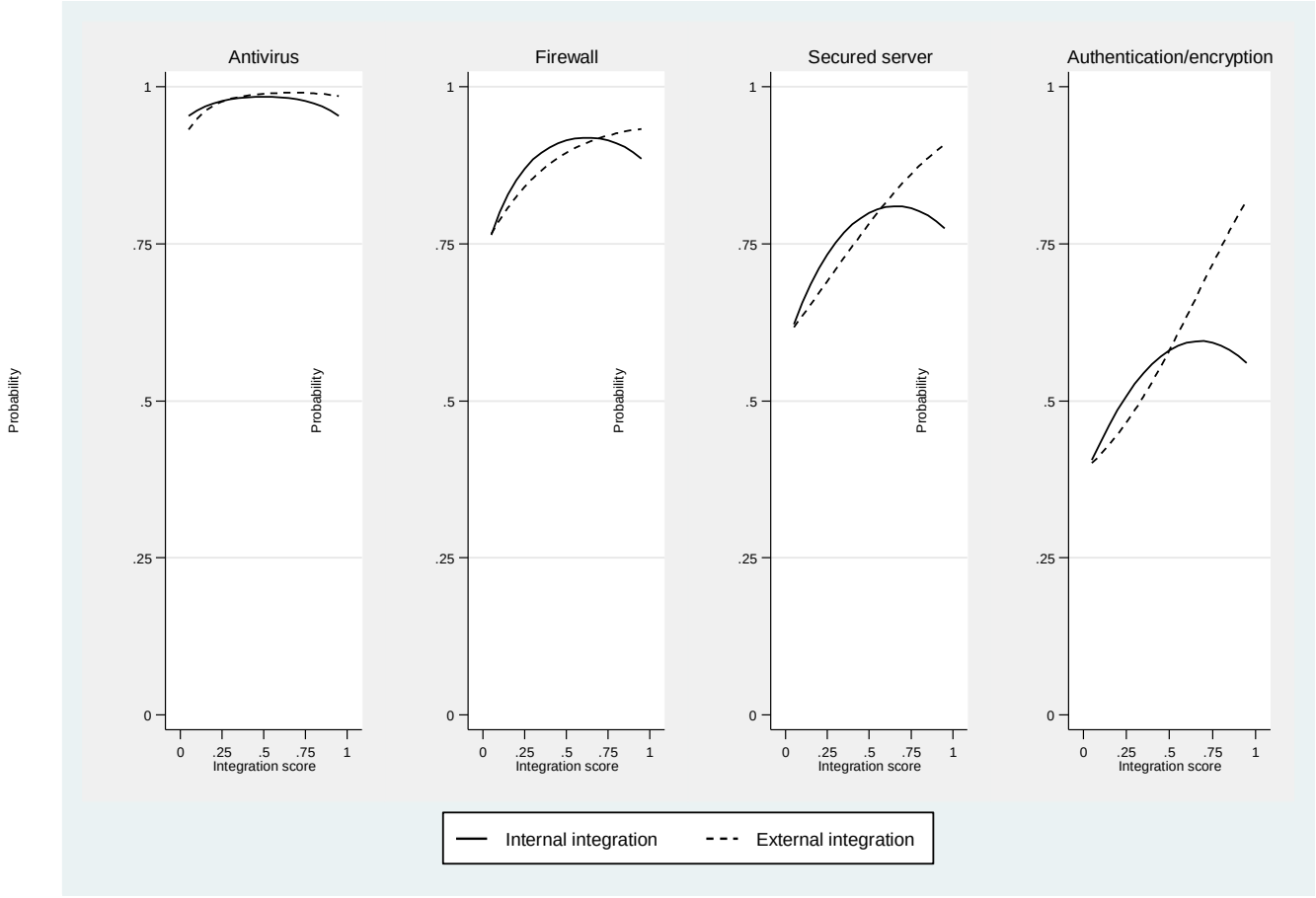

Figure 6. Dose-Response Function for Each Cybersecurity Tool as a Function of Integration

Source: survey COI-TIC 2006, authors' calculations.

Discussion

The body of evidence above indicates that increasing information systems integration is being accompanied by increasing attention to acquisition of cybersecurity technologies. As summarized in Table 3, this phenomenon is even more important in settings with external integration than it is in settings with only internal integration. In cases of highly volatile organizational environments, organizations increase their use of self-protective cybersecurity countermeasures, and cybersecurity is hopefully improved as a result of increasing these self-protective countermeasures.

Integration without cybersecurity or with fewer cybersecurity investments due to fewer vulnerability points may no longer be the option. The compromise of an integrated system has great impact. It affects all integrated functions both internal and external. The compromise of a non-integrated system is confined to just one internal, contained system. Our findings suggest that this effect is perceived since it seems that IS integration increases exposure to risk and is associated with cybersecurity countermeasures. The response to greater risk exposure is consistent with an institutional explanation insisting on the role played by vendors in the commoditization of security technologies (Stewart, 2005). It is also consistent with the notion that cybersecurity has now become a functional requirement by making it a specific system goal (D'Aubeterre et al., 2008).

Another reason why integration is highly correlated with cybersecurity may be that both require a certain level of IT sophistication. Several of the contingency or control factors explaining cybersecurity countermeasures may also be simply reflecting IT or organizational sophistication. Indeed, Raymond et al. (1995) included *diversity of IT* used and *application of integration* in the same *IT usage sophistication* construct. The correlation between internal IS integration and external IS integration (De Corbière et al., 2012) can also reflect IS sophistication or be related to IS maturity. Internal IS integration and external IS integration are influenced by numerous common contingency factors (De Corbière et al., 2012). Arguably, IS sophistication and IS maturity are broader than IS integration and could even be treated as antecedents to IS integration. In such models, it would be interesting to see if H2 still holds and what would be the best explanations.

Our results on H1 also contribute a contrasting view to the assumption that IS integration reduces cybersecurity investment needs. Instead, we find that higher degrees of integration appear to entail simultaneously improving organizational cybersecurity (or vice-versa). This finding is consistent with current initiatives in the oil and gas industry by Qian et al. (2012) as well as with opinions expressed in the operations and supply chain management literature, although without the empirical evidence in our study (Smith et al., 2007). Our vulnerability theory and risk exposure perspective supports an interpretation of this result as reflecting a sensitivity to the transition from a large set of uncontrollable vulnerabilities to a smaller set of vulnerability points that entail specific, feasible countermeasure technologies.

Table 3. Summary of the Hypotheses and the Evidence

Hypotheses	Evidence	Findings / Interpretation
H1. The greater the IS is integrated, the more the firm will invest in technology for self-protection cybersecurity countermeasures in the firm's information system.	Supported	Very robust finding across all analyses. IS integration leads to fewer vulnerability points while potential impact of a breach increases. Conjoint effect makes security spend both needed and more manageable.
H2. The positive relationship between integration and cybersecurity spend (**H1**) will be stronger when considering external IS integration rather than internal IS integration.	Supported	This finding appears only when contingency factors are controlled for in the econometric analysis. For external IS integration, vulnerability points involve higher risk exposure because uncertainty is higher.
H3. In highly volatile environments, firms will use a greater diversity of self-protective cybersecurity countermeasures than in less volatile environments.	Supported	This finding appears clearly from Table 2, although the effect is not very strong. Environmental volatility can affect all three fundamental aspects of vulnerability. Conceptually, this means vulnerability point requirements must be more elaborate to address these aspects.

The positive correlation between IS integration and the spend for security countermeasures applies to both internal and external integration. However, we find that this correlation is stronger for external integration. This finding is consistent with calls for more attention to risks inherent in extending the enterprise view of risk management in cases where risks are inherited from business partners in the supply chain (Sutton, 2006). In the supply chain, information sharing and partner relationships are designed to drive down supply chain risk (Christopher & Peck, 2004). However, for Smith et al. (2007), the high integration of the supply chain and IT requirements essential to this goal can increase risk, as greater levels of collaboration expose significantly more sensitive information to potential risk from a wider variety of sources.

In support of this assertion, Smith et al. (2007) found indications that highly integrated supply chains were at greater risk likelihood for security incidents versus those exhibiting less integration. While these indications were not rigorously tested in the aforementioned paper, when there is greater awareness of such incidents, we argue that firms will invest in IS integration for their supply chains because of the fewer and more controllable vulnerability points and will in parallel invest in security countermeasures to pursue their effort in driving down supply chain risk. We provide empirical evidence that organizations are responding accordingly and offer an alternative model for how this response becomes formulated.

Our theory attributes the diversity of cybersecurity countermeasure technologies to the dynamic nature of vulnerabilities in volatile environments. In volatile settings, cybersecurity countermeasure technologies are needed to address all three types of vulnerability conditions: threat capability, system susceptibility, and threat accessibility. Finally, volatility is positively correlated with the spend for cybersecurity countermeasures. Some authorities call for cybersecurity spend following system integration to replace legacy security that is obsolesced by integration (Tracy, 2007). Our study offers an alternative and empirically based explanation and strategy based on the new vulnerability points created by system integration.

In the broadest sense, our study explains the mechanism by which system integration is itself a risk treatment. Non-integrated systems with a large constellation of uncontrolled vulnerabilities often denote an organizational asset with an exposure to risk best characterized as “avoidance.” Such systems have a high likelihood of high-impact losses. Integration offers the means by which an organization can retire such systems, i.e. replacing them with one having a more controllable risk constellation. In the study above, we explain exactly how these controllable risks (vulnerability points) arise from integrated systems.

Regarding contribution to practice, our results contribute evidence to support cybersecurity managerial strategies that more integrated enterprise systems require not less cybersecurity spend, but more spend on cybersecurity countermeasure technology, at least in terms of the number of different kinds of countermeasures. Further, our findings complement this requirement by implying a greater level of cybersecurity countermeasures in more integrated settings. Such a strategy is consistent with calls to increase security in ERP environments across the board (van Holsbeck & Johnson, 2004). Firms will strive to further integrate their systems and concomitantly implement IT security countermeasures that have been made more valuable and identifiable. The benefits of the integration are clarified through the justification for controllable vulnerability points. However, such strategy contrasts concerns that ERP systems are becoming highly vulnerable as Internet connectivity opens potential access compromises to such integrated systems (She & Thuraisingham, 2007).

As an IS study, our research aim centralized the acquisition of cybersecurity countermeasure technologies in settings where systems are integrated. Accordingly, we are centrally concerned with vulnerability points that arise in such settings in a form for which self-protection treatments are justified. We did not collect data regarding the possibility that new vulnerability points might appear in a form where risk transfer or self-insurance treatments would be more suitable as illustrated in Figure 7.

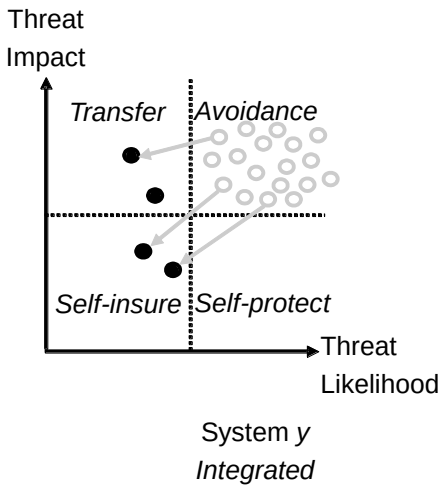

Figure 7. Possible Further Effect of Integration on the Risk Management Situation

For cybersecurity countermeasures, self-protection treatments often involve cybersecurity technologies.

As with other arenas for risk management, self-insurance and risk transfer will more likely invoke financial treatments, such as business interruption insurance and corporate financial reserves. The scope of our study did not extend beyond technologies. Future research is needed to investigate whether system integration also generates new vulnerability points in the other two quadrants of risk treatment.

Risk-transfer and self-protection are not mutually exclusive because many risk-transfer countermeasures (e.g., insurance) do not eliminate the need for self-protection (e.g., access control) (Furnell & Dowland, 2000). Good management will balance self-protection and risk-transfer efforts for the setting. Too much emphasis on self-protection will result in underdevelopment of risk-transfer and leave an organization poorly prepared to deal with the rarer, but more unpredictable high-impact incidents (Jajodia et al., 1999). Highly integrated information systems in volatile environments increase these effects by exposing fewer, but more critical, vulnerability points.

The theoretical interpretation that in response to greater system integration, self-protecting strategies would be privileged, would be strengthened and offer indications on cybersecurity strategy if future research developed relevant data on cybersecurity outsourcing, insurance and other tactics for risk transfer. Such future research could investigate specific cybersecurity clauses to assess the effectiveness of risk transfer. The model above considers only self-protective countermeasures, but our theorization could be extended to test risk-transfer countermeasures beyond outsourcing, such as insurance. This distinction between self-protection and risk-transfer has also long been in the assumption space of security planners. The theoretical distinction is anchored to the occurrence of a security incident (Baskerville et al., 2014). Upon such an occurrence, there is a pivot in the management activities from self-protection to risk-transfer.

This is a national survey that could not pursue many ideal questions related to information security policy and/or behavior. Respondents provide a top management perspective on these issues. Future research might test whether operational security managers would respond similarly. Our study also operationalizes an increase in cybersecurity as an increase in the number of cybersecurity countermeasures. This equivalence would not hold in situations where countermeasures are misconfigured or obsolete. The practical issues of survey length required the use of very broad categories of technologies, such as the combination authentication/encryption, that stretched across access control authentication, digital signature authentication, and data encryption. Future research could explore whether it would be meaningful to investigate the relationship between integration and each of these technologies discretely.

In our empirical specification, we examine the relationship between cybersecurity countermeasures and integration by first assuming that integration is an exogenous decision. However, this assumption is unlikely to hold as firm characteristics like size or sector of activity will themselves have an influence on the firm decision to integrate less or more, either internally or externally. We decide to turn to a selection on observables framework to account for endogeneity. As there is no relevant instrument to endogeneize the level of integration, we treat the score of integration as a continuous treatment and estimate a generalized propensity score to calculate dose-response functions. In doing so, we are unable to account for selection due to unobserved heterogeneity. If there are some unobserved characteristics of firms in our data set which influence both the level of integration and the decision to adopt some cybersecurity countermeasures, then our estimates will be biased. Being able to track firms over time using longitudinal data would be useful to study the relationship between changes in integration over time and changes in the adoption of cybersecurity tools.

Future research is needed to see if these results hold in other countries where there is wider adoption of consumerized IT (Koch et al., 2014). Enterprise systems are typically integrated systems; these are highly common in France where the study was conducted. For instance, the use of smartphones, tablets, and similar nomadic equipment with internet and ubiquitous computing lends itself to the Bring-Your-Own-Device trend. Systems with such equipment are notoriously well integrated yet difficult to secure (Monroe, 2010).

There are other areas of future research that arise as a result of this study. For example, research is needed to investigate whether this correlation between cybersecurity countermeasures and IS integration matters from an economic performance viewpoint, and if it is contingent on the external and internal environment of the firm. They may be overly dependent on self-protective countermeasures where risk-transfer countermeasures would be more economical. Alternatively, there may be a need to revise findings from existing research on the ideal mix of self-protective countermeasures versus risk-transfer countermeasures in differing settings.

Conclusion

The study reported above makes a strong and novel contribution to the existing literature. It offers empirical evidence that IS integration is positively correlated with cybersecurity countermeasures and that this relationship is all the stronger when we consider external integration. The representativeness of the sample, the ability to take into account volatility and numerous control variables such as various organizational and infrastructural characteristics as well as potential selection bias and endogeneity, and the in-depth econometric analysis confer to the findings high external validity and provide credible empirical evidence in a domain where such evidence is rare (Siponen et al., 2008). Finally, the argument that IS integration is in itself a risk avoidance mechanism transforming systems into sufficiently or more controllable assets to add on cybersecurity spend is a theoretical contribution.

Notes

[1] This point might hold when software designers' efforts reduce the attack surface of enterprise systems (Manhadata & Wing, 2011).

[2] Most of the time, the survey was filled in by the CIO, or in small firms by the member of the Top Management Team overlooking IT issues.

[3] The fact that the survey was conducted by INSEE, a national administration well-known by firms for its code of ethics and for its professionally trained representatives, and was presented as mandatory explains why so many firms answered the questionnaire even with sensitive questions such as those on security.

[4] For practical reasons of questionnaire length, the authentication/encryption item encompasses a broad range of cryptographic and access control technologies that protect confidentiality, integrity and availability. This includes access control authentication such as pin codes and passwords, digital signature authentication (on both data and security software), and data encryption for both transmission and storage.

[5] This multivariate statistical technique is used to reduce the number of variables into a small number of dimensions that capture the common information most successfully. When there is a high degree of correlation among the selected variables, then only a few components are required to pick up common information.

[6] Let I_{int} and I_{ext} be the indices of internal and external integration, respectively. Since I_{int} and I_{ext} do not cover the same interval (I_{int} ranges from -2.33 to 5.34 and I_{ext} from -2.55 to 5.02), we chose to normalize these indices so that $I_{\text{int}} \in [0;1]$ and $I_{\text{ext}} \in [0;1]$. The normalized indices I_{int}^{N} and I_{ext}^{N} are $I_{\text{int}}^{\text{N}} = (I_{\text{int}} - \min(I_{\text{int}}))/(\max(I_{\text{int}}) - \min(I_{\text{int}}))$ and $I_{\text{ext}}^{\text{N}} = (I_{\text{ext}} - \min(I_{\text{ext}}))/(\max(I_{\text{ext}}) - \min(I_{\text{ext}}))$.

[7] The difference in coefficients of correlation is statistically significant for firewall (with a test statistic equal to 4.224). The correlation is higher for internal integration (0.283) than for external integration (0.242).

[8] For the sake of robustness, we have also estimated a joint model comprising one ordered Probit equation for number of tools and a quadrivariate Probit model for the four tool-specific dependent variables. As the model requires the calculation of a five-dimensional normal integral, we rely on a simulation method based on the Geweke-Hajivassiliou-Keane algorithm (Gates, 2006). These additional results, which are available upon request, lead to very similar conclusions.

[9] By definition, faster connections increase potential threats and vulnerability so that additional cybersecurity countermeasures are needed.

[10] Endogeneity may also be due to measurement errors. Since integration is a composite indicator stemming from a large set of outcomes, problems due to measurement errors for some components of integration are presumably lessened given the use of a principal component analysis. We do assume that top IT managers (who provide answers to the survey) are competent in their organization's IT functionality, security processes, and countermeasures.

[11] For antivirus, the slope is also steeper for external integration than for internal integration but only in the first half of the distribution of integration score. We have also estimated dose-response functions with each cybersecurity outcome expressed as a quadratic function of the treatment level (rather than linear). We observe a reduction in secured servers and authentication with very high internal integration, above the 9th decile of integration score. For very high levels of internal integration, it may be that system susceptibility and threat accessibility get so low that, despite the attractiveness of target and the gravity of risk, the exposure to risk is lower.

References

Aubert, B., Patry, M., & Rivard, S. (1998). *Assessing the risk of IT outsourcing*. Paper presented at the *31st HICSS* Hawaii International Conference on Systems Science, IEEE.

Aubert, B., Patry, M., & Rivard, S. (2005). A framework for information technology outsourcing risk management. *The Data Base for Advances in Information Systems*, *36*(4), 9-28.

Austin, P.C., (2011). An introduction to propensity score methods for reducing the effects of confounding in observational studies. *Multivariate Behavioral Research*, *46*(3), 399-424.

Bahill, A.P., & Smith, E. (2009). An industry standard risk analysis technique. *Engineering Management Journal, 21*(4), 16-29.

Barki, H., Rivard, S., & Talbot, J. (1993). Towards an assessment of software development risk. *Journal of Management Information Systems*, *10*(2), 203-225.

Baskerville, R. (1991). Risk analysis: An interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems, 1*(2), 121-130.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management, 51*(1), 138-151.

Beretta, S. (2002). Unleashing the integration potential of ERP systems: The role of process-based performance measurement systems. *Business Process Management Journal*, *8*(3), 254-277.

Besson, P., & Rowe, F. (2001). ERP project dynamics and enacted dialogue: Perceived understanding, perceived leeway and the nature of task-related conflicts. *The Data Base for Advances in Information Systems*, *33*(4), 47-66.

Bia, M., & Mattei, A. (2008). A Stata package for the estimation of the dose-response function through adjustment for the generalized propensity score. *Stata Journal*, *8*(3), 354-373.

Bidan, M., & Rowe, F. (2004). *Urbanization practices and strategic behavior: Openness of architecture and enactment in two medium sized companies*. Paper presented at the 9th Conference of the Association Information Management, Evry, France.

Bidan, M., Rowe, F., & Truex, D. (2012). An empirical study of IS architectures in French SMEs: Integration approaches. *European Journal of Information Systems, 21*(3), 287-302.

Boehm, B. (1989). Software risk management. In C. Ghezzi & J.A. McDermid (Eds.), *Lecture Notes in Computer Science*, *Vol. 387* (pp. 1-19). Springer, Berlin, Heidelberg.

Brumley, D., Newsome, J., Song, D., Wang, H., & Jha, S. (2008). Theory and Techniques for Automatic Generation of Vulnerability-Based Signatures. *IEEE Transactions on Dependable and Secure Computing, 5*(4), 224-241.

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management*, *15*(2), 1-14.

D'Aubeterre, F., Singh, R., & Iyer, L. (2008). Secure activity resource coordination: Empirical evidence of enhanced security awareness in designing secure business processes. *European Journal of Information Systems, 17*(5), 528-542.

De Corbière, F., Rowe, F., & Wolff, F.C. (2012). De l'intégration interne du système d'information à l'intégration du système d'information de la chaîne logistique. *Systèmes d'Information et Management*, *16*(1), 81-111.

Fisher, R. (1984). *Information Systems Security*. Englewood Cliffs: Prentice-Hall.

Furnell, S.M., & Dowland, P.S. (2000). A conceptual architecture for real-time intrusion monitoring. *Information Management & Computer Security, 8*(2), 65-75.

Galbreth, M., & Shor, M. (2010). The impact of malicious agents on the enterprise software industry. *MIS Quarterly*, *34*(3), 595-612.

Gates, R. (2006). A Mata Geweke–Hajivassiliou–Keane multivariate normal simulator. *Stata Journal, 6*(2), 190-213.

Guardabascio, B., & Ventura, M. (2014). Estimating the dose-response function through a generalized linear model approach. *Stata Journal*, *14*(1), 141-158.

Heckman, J., Ichimura, H., & Todd, P. (1998). Matching as an econometric evaluation estimator. *Review of Economic Studies, 65*(2), 261–294.

Hirano, K., & Imbens, G. W., (2004). The propensity score with continuous treatments. In A. Gelman & X.-L. Meng (Eds.), *Applied Bayesian Modeling and Causal Inference from Incomplete-Data Perspectives* (pp. 73–84). West Sussex: Wiley Interscience.

Huang, S., & Han, W. (2008). Exploring the relationship between software project duration and risk exposure: a cluster analysis. *Information and Management*, *45*(3), 175-182.

Hughes. J., & Cybenko, G. (2014). Three tenets for secure cyber-physical system design and assessment. In I. V. Ternovskiy & P. Chin (Eds.), *Cyber Sensing 2014: SPIE Defense+ Security* (Vol. 9097, pp. 90970A-90915). International Society for Optics and Photonics.

ISO/IEC. (2013). ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management (International Standard No. ISO/IEC 27002:2013). Geneva: International Standards Organization

Jajodia, S., McCollum, C.D., & Ammann, P. (1999). Trusted recovery. *Association for Computing Machinery. Communications of the ACM 42*(7):71-75.

Jolliffe, I.T. (2002). *Principal Component Analysis*, Springer.

Jones, A., & Ashenden, D. (2005). *Risk Management for Computer Security: Protecting Your Network & Information Assets*. Oxford: Butterworth-Heinemann.

Keats, B.W., & Hitt, M.A. (1988). A causal model of linkages among environmental dimensions, macro organizational characteristics, and performance. *Academy of Management Journal, 31*(3), 570-598.

Kim, D., Kavusgil, S.T., & Calantone, R.J. (2006). Information systems innovations and supply chain management: Channel relationships and firm performance. *Journal of the Academy of Marketing Science, 34*(1), 40–54.

Koch, H., Zhang, S., Giddens. L., Milic, N., Yan, K., & Curry, P. (2014). *Consumerization and IT Department conflict*. Paper presented at the International Conference on System Sciences, Auckland, New Zealand.

Kotulic, A., & Clark, J. (2004). Why there aren't more information security research studies. *Information and Management, 41*(5), 597-607.

Lairet, G., Geoffroy, B., & Rowe, F. (2016). *Understanding the undesirable effects of using interorganizational systems and integrated information systems: Case studies among supply chain partners*. Paper presented at the European Conference on Information Systems, Istanbul, Turkey.

Lee, H., & Larsen, K. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

Leifer, R. (1989). Understanding organizational transformation using a dissipative structure model. *Human Relations, 42*(10), 899-916.

Manadhata, P., & Wing, J. (2011). An attack surface metric. *IEEE Transactions on Software Engineering, 37*(3), 371-386.

Marciniak, R., El Amrani, R., Rowe, F., & Adam, F. (2014). Does ERP integration foster Cross-Functional Awareness? Challenging conventional wisdom for SMEs and Large French firms. *Business Process Management Journal, 20*(6), 865-886.

Markus, M.L. (2001). Reflections on the system integration enterprise. *Business Process Management Journal*, *7*(3), 1-9.

McDermott, J., & Fox, C. (1999). *Using abuse case models for security requirements analysis, Paper presented at the Computer Security Applications Conference.* (ACSAC '99) Proceedings. 15th Annual 1999: 55-64.

Monroe, I. (2010). Worms in the Apple? *ABA Journal, 96*(3), 33.

Nappa, A., Rafique, M.Z., & Caballero, J. (2015). The MALICIA dataset: Identification and analysis of drive-by download operations. *International Journal of Information Security, 14*(1), 15-33.

Oladimeji, E.A., Chung, L., Jung, H.T., & Kim, J. (2011). *Managing security and privacy in ubiquitous eHealth information interchange*. Paper presented at the 5th International Conference on Ubiquitous Information Management and Communication, Seoul, Korea.

Olhager, J., & Selldin, E. (2003). Enterprise resource planning survey of Swedish manufacturing firms. *European Journal of Operational Research, 146*(2), 365-373.

PCI Security Standards Council. (2016). *PCI DSS Requirements and Security Assessment Procedures, Version 3.2*. Wakefield Mass: PCI Security Standards Council.

Qian, Y., Fang, Y., & Gonzalez, J. (2012). Managing information security risks during new technology adoption. *Computers and Security*, *31*(8), 859-869.

Rajaguru, R., & Matanda, M. (2013). Effects of inter-organizational compatibility on supply chain capabilities: Exploring the mediating role of inter-organizational information systems (IOIS) integration. *Industrial Marketing Management, 42*(4), 620-632.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121-139.

Raymond, L., Paré, G., & Bergeron, F. (1995). Matching information technology and organization structure: An empirical study with implications for performance. *European Journal of Information Systems*, *4*(1), 3-16.

Robles, F. (2011). Export channel integration strategy and performance: A contingency approach. *International Journal of Business and Management, 6*(12), 3-12.

Sharif, A., & Irani, Z. (2005). Emergence of ERPII characteristics within an ERP integration context. *American Conference on Information Systems*, Omaha, USA.

She, W., & Thuraisingham, B. (2007). Security for Enterprise Resource Planning Systems. *Information Systems Security*, *16*(3), 152-163.

Siponen, M., Willison, R., & Baskerville, R. (2008). *Power and practice in information systems security research.* Paper presented at the 29th International Conference on Information Systems, Paris, France.

Smith, G.E., Watson, K.J., Baker, W.H., & Pokorski, J.A. (2007). A critical balance: Collaboration and

security in the IT-enabled supply chain. *International Journal of Production Research, 45*(11), 2595-2613.

Steiger J.H., (1980). Tests for comparing elements of a correlation matrix. *Psychological Bulletin*, 87, 195-201.

Steiger, J.H. (2005). Comparing correlations: Pattern hypothesis tests between and/or within independent samples. In A. Maydeu-Olivares & J.J. McArdle (Eds.), *Contemporary Psychometrics: A Festschrift in Honor of Roderick P. McDonald* (pp. 371-408). Mahwah.

Stewart, A. (2005). Information security technologies as a commodity input. *Information Management & Computer Security, 13*(1), 5-15.

Straub, D.W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255-276.

Straub, D.W., & Welke, R. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Suleiman, H., & Svetinovic, D. (2013). Evaluating the effectiveness of the security quality requirements engineering (SQUARE) method: A case study using smart grid advanced metering infrastructure. *Requirements Engineering, 18*(3), 251-279.

Sun, L., Srivastava, R.P., & Mock, T.J. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems, 22*(4), 109-142.

Sutton, S. G. (2006). Extended-enterprise systems' impact on enterprise risk management. *Journal of Enterprise Information Management, 19*(1/2), 97-114.

Tanriverdi, H., Rai, A., & Venkatraman, N. (2010). Reframing the dominant quests of information systems strategy research for complex adaptive business systems. *Information Systems Research, 21*(4), 822-834.

Tracy, R. P. (2007). IT security management and business process automation: Challenges, approaches, and rewards. *Information Systems Security, 16*(2), 114-122.

Van Everdingen, Y., Van Hillegersberg, J., & Waarts, E. (2000). Enterprise Resource Planning: ERP adoption by European midsize companies. *Communications of the ACM*, *43*(4), 27-31.

Van Holsbeck, M., & Johnson, J. Z. (2004). Security in an ERP World. Online report. Downloaded from http://hosteddocs.ittoolbox.com/MH043004.pdf. 26 Oct 2015.

Venkatraman, N. (1994). IT-enabled business transformation: From automation to business scope redefinition. *Sloan Management Review, 35*(2), 73-87.

Wada, H., Suzuki, J., & Oba, K. (2008). A model-driven development framework for non-functional aspects in service oriented architecture. *International Journal of Web Services Research, 5*(4), 1-31.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*(2),101-105.

Yee, K.P. (2004). Aligning security and usability. *IEEE Security & Privacy*, *2*(5), 48-55.

Xue, L., Ray, G., Gu, B. (2011). Environmental uncertainty and IT infrastructure governance: A curvilinear relationship. *Information Systems Research*, *22*(2), 389-399.

Zellner, A. (1962). An efficient method of estimating seemingly unrelated regression equations and tests for aggregation bias. *Journal of the American Statistical Association, 57*(298), 348-368.

About the Authors

Richard Baskerville is Regents' Professor and Board of Advisors Professor of Information Systems at Georgia State University and Professor in the School of Information Systems at Curtin University, Perth, Australia. His research regards security of information systems, methods of information systems design and development, and the interaction of information systems and organizations. Baskerville is editor emeritus of the *European Journal of Information Systems*. He is a Chartered Engineer, and holds a BS *summa cum laude* University of Maryland, MSc and PhD London School of Economics, PhD (*hc*) University of Pretoria, and DSc (*hc*) Roskilde University.

Frantz Rowe is Professor of Information Systems at University of Nantes and at SKEMA Business School. He was trained as an engineer (ME UC Berkeley and ENTPE) and as an economist (Université de Lyon). He holds a PhD from Université de Paris in MIS. He is Co-Editor of the *European Journal of Information Systems* and is a Fellow of the AIS. His principal research interests pertain to organizational transformations, especially as related to enterprise systems projects and use. His interests also include philosophy and information systems.

François-Charles Wolff is Professor of Economics at the University of Nantes, France. He received a PhD in Economics from the University of Nantes in 1998 and is Agrégé des Universités since 2004. He is in the scientific board of the *Revue Economique* and *Economie et Statistique*. He is author and co-author of 150 peer-reviewed articles dealing with applied microeconometrics.

Appendix. Questionnaire Items

● *Cybersecurity questions*
Does you firm use the following cybersecurity countermeasures?
- Self-protection or control software against viruses? Yes/no
- Firewalls (hardware or software)? Yes/no
- Secured servers (using protocols such as https)? Yes/no
- Authentication mechanisms (PIN codes, data encryption, digital signature)? Yes/no.

● *Internal integration*
The internal integration synthetic indicator is based on the following questions providing 11 responses:
- which type of IT application does your firm use **for each** of the **six** following functions : R&D, purchase, sales, production, human resources, accounting departments ?
    - ERP: yes/no
    -
- is your firm equipped with central databases in the following domains?
    - R&D: yes/no
    - sales: yes/no
    - human resources: yes/no
    - accounting: yes/no
- does you firm use tools for interconnecting databases and applications such as an Enterprise Integration Application or a Service Oriented Architecture? Yes/no

● *External integration*
The external integration synthetic indicator is based on the 12 following questions:
- does your firm use an extranet? Yes/no
- does your firm use of an EDI? Yes/no
- does your firm use of tracking tools? Yes/no
- does your firm use a purchasing/sales delivery systems coupled with internal systems for supplies? Yes/no
- does your firm use a purchasing/sales delivery systems coupled with internal systems for billing and payments? Yes/no
- does your firm use a purchasing/sales delivery systems coupled with internal systems for operations? Yes/no
- does your firm receive orders through internet? Yes/no
- does your firm receive orders through EDI? Yes/no
- does your firm place orders through internet? Yes/no
- does your firm place orders through EDI? Yes/no
- does your largest client have its system coupled with that of the firm for orders and billing? Yes/no
- does your firm have its system coupled with its largest suppliers for orders and billing? Yes/no.

● *Internal dynamism*
The Internal Dynamism synthetic indicator is based on the following two questions providing five dummies:
- since 2003, your firm has undertaken the following:
    - financial restructuring (merger, acquisition, sale, buy-out): yes/no
    - organizational chart restructuring: yes/no
    - offshore relocation of part of its activity: yes/no
    - locating new sites abroad (without relocation): yes/no
- what is the strategic importance of the novelty of your products or services? Null or very low, low, strong, very strong