

WHITE PAPER

Innovation and Security: Collaborative or Combative

Sponsored by: RSA

Christian A. Christiansen

September 2008

IDC OPINION

Business innovation is a very important part of business strategy and increasingly a critical component to keeping a competitive edge over rivals. It is the sheer strategic importance of innovation that causes increased concern about information security's contribution to the stifling and smothering of business innovation.

In response to these concerns, IDC embarked on a study to further understand the relationship between information security and business innovation. Our research found that:

- ☒ The majority of senior executives believe it is critical to create an environment for business innovation within their companies.
- ☒ When considering business innovation, respondents find utilizing joint ventures as the most important way to innovate followed by enhanced business performance and governance.
- ☒ All respondents are highly confident of their risk assessment capabilities when it comes to business innovation initiatives, but only around 20% rate themselves extremely effective.
- ☒ Respondents believe IT Security risk is the single biggest inhibitor to business innovation, with more than 80% of the executives surveyed admitting their organizations have "occasionally" or "often" backed away from innovative business opportunities because of information security concerns.
- ☒ The majority of organizations consider themselves "compliance/control driven" when it comes to security; with only 21% reporting that their security efforts are strategic, proactive and using security to enable innovation.
- ☒ Among the largest companies, respondents believe IT security should report directly to the CEO. In addition, organizations commonly feel that information security is a board level issue.
- ☒ C-level executives indicate business alignment of information security as a high priority, yet the compliance or fear driven nature of many organizations reveals the disconnect between the desired and actual state.

The majority of respondents (61%) consider themselves "Compliance/control driven (implementing checklist controls, focused on passing audits, trying to create efficiencies to drive down the costs of compliance)." Other IDC surveys show that compliance failures are the single biggest risk to business today.

As for the positive elements, only 21% said that they would characterize security in their organizations as, "Acceleration/Confidence (proactive, business aligned, risk based, strategic, using security to enable innovation)."

IDC believes companies need to find a succinct balance addressing the spectrum of their business needs, not just business innovation and the information security that has the potential to stifle it. The successful companies will find a way to leverage the strengths of both to gain a competitive edge over those companies who ignore one in favor of the other.

TABLE OF CONTENTS

	P
Methodology	1
This Research	1
Key Research Findings.....	1
Business Innovation	1
Security and Compliance.....	2
Sharing Risk	2
Continued Challenges	3
Engaging Senior Management	4
Strategies and Solutions.....	4
Survey Results and Analysis	5
Demographics	5
Primary Business/Industry	5
Gross Annual Revenues.....	6
Job Titles	7
Company Size	7
Survey Summary	7
Where Primary Responsibility Sits for Driving Innovation	7
Importance Of Creating An Innovation Environment	8
Importance of an Information Security Leadership Function that can Enable and Impact C-Level Business Priorities	10
Top Five Barriers to Innovation.....	13
Measuring Information Security Leadership on Business Growth and Innovation.....	14
Types of Innovative Initiatives Pursued and/or Funded Over the Next 18 to 24 Months by Company Revenue	17
Rating the Effectiveness of Respondents' Organizations at Assessing the Information Risk Associated with Potential Innovation.....	18
Assertive, Compliant or Fearful Organization Descriptions	19
Frequency of Organizational Shying Away from Innovative Business Initiatives Because of Potential Information Risks.....	21
Potential Consequences of Excluding Information Security in the Innovation Process	22
Information Security Team Engaged in Business Innovation Initiatives.....	24
Information Security Function's Impact on Innovation Process	27
Reporting Structure of Most Senior Information Security Individual.....	28
Board Level Importance of Information Security.....	29
Selling Information Security to Executive Leadership.....	30
Successful Strategies in Getting Information Security Involved with Innovation.....	30
What Can Vendors Do?.....	31
Services Above and Beyond Day to Day Activities Provided by the Information Security Organization	32
Key Findings In Verbatim Questions.....	34
Verbatim Question 1: Define 'business innovation' in your market or organization.....	34
Verbatim Question 2: What things is the information security team at your organization doing to enable innovation?	35
Verbatim Question 3: Please share any additional comments or thoughts you might have on security's impact on business innovation.....	35

TABLE OF CONTENTS — Continued

	P
Define 'business innovation' in your market or organization? (based on Verbatim Question 1).....	36
Vendors can help their customers reach their goals by:	36
Conclusion	36

LIST OF TABLES

	P
1 Gross Annual Revenue	6
2 How Security Impacts Their Organization	6
3 Job Titles.....	7
4 Importance of Creating an Innovation Environment	9
5 Security Effect On Business Innovation	9
6 Security Effect On Business Innovation by Title.....	10
7 Importance of Having Leaders in the Information Security Function Who Can Enable and Impact C-Level Business Priorities.....	11
8 Importance of Having Security Leaders Influence C Level Decisions	11
9 Responses by Function.....	12
10 C Level BOD Level Responses	12
11 Primary Responsibility for Driving Business Innovation	15
12 Innovation Tied to Performance	15
13 Security/IT or LOB the Top Five Initiatives Over Next 18 to 24 Months	16
14 Assessing Risk Of Potential Innovation.....	18
15 Effectiveness Based on Opinion	19
16 Issues Driving Security Strategies.....	19
17 Impressions Of Security	20
18 Shying Away from Innovative Business Initiatives Due to Information Risks	21
19 Impressions Of Shying Away from Innovations Because of Information Risks.....	22
20 When Is Information Security Engaged In Business Innovation Initiatives?	24
21 Opinions of When Security Should be Brought in on Business Innovations.....	26
22 LOB and Security/IT Opinions of when security should be brought in on business innovations.....	26
23 Information security function impact on the innovation process	27
24 Most Senior Security Staff Reporting	28
25 Who Should the Most Senior Security Staff Report to?.....	29
26 Opinions On Whether Information Security Is a Board-Level Issue	30

LIST OF FIGURES

P

1	Organizational Effectiveness at Assessing Information Risk Associated with Potential Innovation	3
2	Respondents by Industry	5
3	Person Responsible for Driving Innovation within Organization	8

METHODOLOGY

The goal of this research was to measure IT Security's affect on business innovation, and to examine if there are ways to change the relationship. This research was conducted by IDC and funded by the RSA division of EMC corp.

IDC and RSA designed the survey to measure the effect of IT security on business innovation. The survey was conducted online by IDC and following the data collection the analysis took place in Q2 2008. Respondents were provided with IDC's definition of "business innovation" and were asked to refer to it when considering each question on the survey.

Respondents to the survey were screened for their direct involvement in IT security, and they include senior management and line of business managers. Approximately 200 individuals were screened and qualified to complete the survey (n = 197). These individuals work for some of the largest companies and are predominantly senior-level employees within their company. For example:

- 80% of respondents' company revenues are \$1B or above
- 73% of respondents are VP executives or above
- 60% of respondents' companies have 5000 employees or above

Participants in the survey included representation from North America (73%) of the total. Other countries represented include UK (14%), India (2%), Australia (6%), and other (5%).

THIS RESEARCH

This paper presents a summary and analysis of a survey conducted by IDC and RSA, The Security Division of EMC. This comprehensive study was designed with the aim of revealing, understanding, analyzing and presenting the predominant issues relating to perceptions about information security's impact, both positive and negative, on business innovation in the enterprise.

Key Research Findings

Business Innovation

To establish a common understanding and basis for survey participants responding to the survey questions, we defined the term *business innovation* as:

"Enterprise strategies to enter new markets, launch new products or services, create new business models, establish new channels or partnerships or achieve operational transformation."

When asked for their definition of business innovation, respondents' exact definitions varied, but the consensus is innovation's goal is to produce new products and services that are more competitive in the market. Key business innovations ranged across the spectrum of market, business and product development strategies – and included new channels, new technologies to support product development, new markets for current products, and new products for current markets.

While there was some emphasis on producing internally-focused innovation to deliver cost savings and greater efficiency, the overwhelming majority expressed the need to describe that next external-facing idea that will produce gains in revenues and profits and will give them the edge over their competition.

Security and Compliance

This research reveals that respondents feel IT Security risk is the single biggest inhibitor to business innovation. This is especially true at the lower-end of the survey's respondents (mid-tier respondents with \$500-\$999M in annual revenues) where three quarters of the respondents cited IT Security as an issue. We believe this IT Security risk is directly related to pressures and demands coming from compliance requirements.

More than 80 percent of the executives surveyed admitting their organizations have occasionally or frequently backed away from innovative business opportunities because of information security concerns. Compliance, with its rigorous regulations and requirements, poses the greatest risk to business innovation. How do people collaborate so they can receive the most information possible, but corporate and customer privacy policies remain enforced? We believe most companies need strong federated authorization and authentication, along with the ability to correlate and analyze possible violations before they occur. Adding to the complexity, increased collaboration using Web 2.0 tools raises the possibility and thus the risk of data breaches and policy violations.

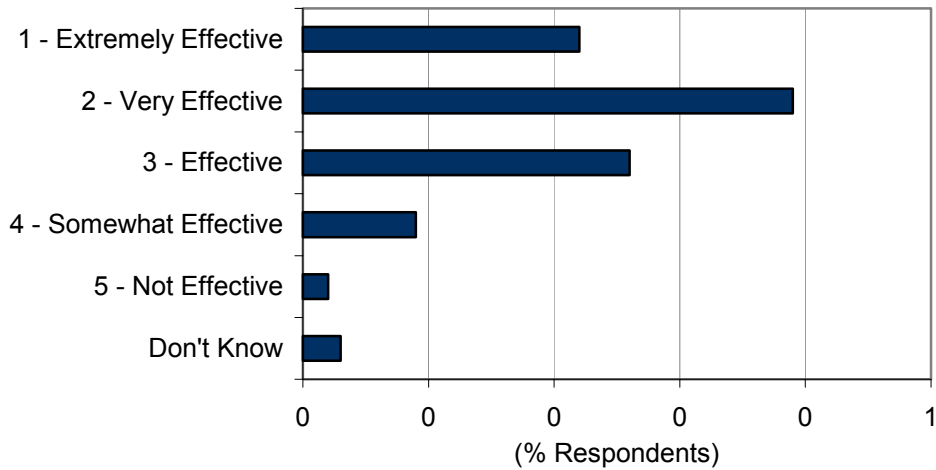
Sharing Risk

Most companies know how to deal with risk at a simple level. When it comes to innovation, however, their tools and processes may be inadequate for new products, services, markets, and partnerships. IDC believes this is the reason only 22% of respondents rate themselves as extremely effective at risk assessment. They don't know what to expect, nor do they know how best to improve their assessment of risk.

FIGURE 1

Organizational Effectiveness at Assessing Information Risk Associated with Potential Innovation

Q. On a scale of 1 to 5 Rate the effectiveness of your organization at assessing the information risk associated with potential innovation.



Source: IDC's Information Security Survey 2008

The importance of joint ventures indicates many companies have internal barriers to business innovation. The IT security organization may be a significant barrier as it increases the complexity required for successful innovation. By seeking joint ventures, IDC believes companies can share risk while reducing the complexity needed to create new successful innovative processes and products.

Continued Challenges

Budgetary constraints are the primary reason organizations allow information security to negatively impact – even stifle – business innovation. The second reason cited was misplaced priorities. Even security/IT respondents agree that confusion over perceived vs. real threats stifles business innovation, indicating there is still a dizzying lack of clarity at the highest decision-making levels on how best to address security threats.

When respondents were asked at what juncture in the innovation process the information security team is typically engaged, the data indicates that while the respondents have good intentions about including security in innovation projects, actual execution against this objective is poor. Whether respondents simply do not think to engage the security team early enough in the development cycle or knowingly exclude security because they feel security teams are too draconian in their rules and restrictions the result is similar - new innovation is stifled by the common pitfall of pulling security in too late, or worse, not including security in the business innovation process at all. Companies are struggling to identify the most effective ways to balance the nurturing of innovation while still retaining effective IT security practices –

however, it has been clearly shown that leaving security to the last minute or not addressing it at all is not the best course of action for any company looking to reduce the impact of security compliance and/or reduce their risk level of security exposure.

Engaging Senior Management

When asked into whom the most senior information security person should report for better integration of information security into the business innovation process, most respondents agree that IT security should report to the CIO level. For the most part, even the security/IT respondents felt they should report to the CIO. Among the largest companies, however, respondents believe IT security should report directly to the CEO. In addition, respondents commonly feel information security is a board level issue.

Interestingly, nearly 80% of CEOs believe security leaders in their organizations are being formally held accountable for their contributions to business growth and innovation. However, survey data indicates that only 44 percent of security leaders believe they are being formally measured on their contributions to business innovation.

Underscoring the perception that senior management still does not understand the real business impact of IT security, many respondents report that the most successful way of "selling" information security, privacy or compliance is through fear-based methods touting compliance penalties, reputation damage, internal/external threats and exposure as well as failed audits (as related to compliance).

Strategies and Solutions

Survey participants were asked to rank the top three strategies they believe are successful in getting information security involved with business innovation. These strategies correlate to the IT security weaknesses relative to the innovation efforts.

The top three strategies respondents felt companies should focus their efforts on are:

- Ensure that the security organization understands the organization's industry and its business goals.
- Ensure that enabling business innovation is either part of the charter or on the scorecard for measuring the information security function.
- Communicate a well-defined roadmap for security that ties directly to corporate strategy and share this road map with other business functions.

When asked how vendors can help integrate IT security into innovation projects, respondents' top answer was: "understand the organization and its particular directions, challenges, and priorities." Specific suggestions included understanding the organizations' verticals, customers, employees, and business unit issues.

SURVEY RESULTS AND ANALYSIS

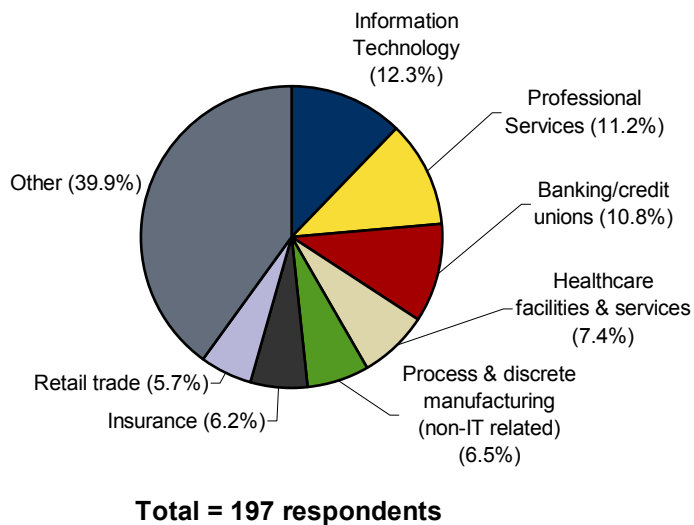
Demographics

Primary Business/Industry

IDC's study surveyed a broad population of respondents, and carefully chose respondents so no one particular industry or company size was dominant in the survey. Therefore, the largest percentage of respondents in a single industry is Financial Services with 21%. However, the rest of the respondents are spread broadly across multiple industries.

FIGURE 2

Respondents by Industry



Source: IDC's Information Security Survey, 2008

When segmented by company size, the \$500M-\$999M group is fairly evenly distributed across all the industries with process/discrete manufacturing holding the largest percentage of 11.7%. The \$1.0 billion - \$4.9 billion group has two strong participants – professional services and information technology – at 14.8% and 14.2% respectively with the remainder distributed across the other segments.

Companies with revenue in the range of \$5 billion - \$20 billion also have a broad distribution across the industry segments, but they are much more concentrated in information technology (15%), construction and professional services (11.1%), and Insurance (10.4%).

Finally, the group of companies with greater than \$20 billion in revenues are heavily concentrated in the banking/credit institutions (31.3%) and insurance (12.9%), the remainder are thinly distributed among a few industries.

Gross Annual Revenues

The survey was designed to disqualify companies below \$500M to provide a concentration on larger enterprises. Respondents are also mostly evenly distributed across their selected function, business line or security/IT, in respect to the distribution of companies by revenue size, see Table 1 below.

TABLE 1

Gross Annual Revenue			
Line of business respondents:	% Responding	Security/IT respondents:	% Responding
Over \$20B	20.40%	Over \$20B	18.80%
\$5 - 20B	34.90%	\$5 - 20B	33.50%
\$1 - 4.9B	26.50%	\$1 - 4.9B	30.30%
\$0.5 - 0.9B	18.20%	\$.5 - .9B	17.50%

n=197
Source: IDC, 2008

Respondents' indications of how security impacts their organizations' innovation are shown below in Table 2.

TABLE 2

How Security Impacts Their Organization					
Positive:	% Responding	Negative:	% Responding	Neutral:	% Responding
Over \$20B	12.70%	Over \$20B	12.90%	Over \$20B	30.60%
\$5 - 20B	37.40%	\$5 - 20B	38.80%	\$5 - 20B	28.40%
\$1 - 4.9B	35.20%	\$1 - 4.9B	34.30%	\$1 - 4.9B	17.70%
\$0.5 - 0.9B	14.70%	\$.5 - .9B	14.00%	\$.5 - .9B	23.40%

n=197
Source: IDC, 2008

Job Titles

When grouped in four categories, CxO (non-IT), CxO (IT/Risk related), Management (non-IT, typically business unit leaders), and Management (IT), there was an even distribution across the four management types. However, the top five respondent titles in terms of percentage of respondents are seen in Table 3:

TABLE 3

Job Titles

Title	% Responding
IT Director	19.20%
CIO	14.10%
President/Owner/Partner	8.60%
Director (non-IT)	7.80%
VP (non-IT)	7.30%

n=197

Source: IDC, 2008

Company Size

The survey contained a good mix of company sizes by employee. We screened by company size to prevent too many smaller company respondents. Specifically, we screened off companies with less than \$500M and less than 1000 employees. If the company qualified on revenue side, we relaxed screener on number of employees.

Survey Summary

Where Primary Responsibility Sits for Driving Innovation

Considering the definition of innovation provided to respondents in the survey, when asked about where the primary responsibility sits for driving innovation in the organization, a third of respondents (34%) indicated executive leadership is responsible. Line of business leadership was ranked second (27%) followed by the CEO leadership and the board of directors (Figure 3).

FIGURE 3

Person Responsible for Driving Innovation within Organization

Q. *Where does the primary responsibility for driving innovation sit within your organization?*



Source: IDC's Information Security Survey 2008

Line Of Businesses (LOBs) have responsibility for driving innovation, but information security also has responsibility for supporting business innovation. This illustrates a basic disconnect between how and possibly when information security is brought into a new innovation project. If innovation is incubated in the line of business and security reports up to senior management (e.g., board of directors, CIO or CEO), then information security will not be aware of new innovation projects until the business line is ready to present its new projects up to the C-level executives.

By the time the LOB is ready to present its projects, the time is often past the point where the security team would have been helpful to the innovation projects. As a result, this disconnect may either cause one or both groups to struggle to "smear" security onto the project retroactively. This could delay the project, increase costs, complicate support, and introduce a high level of risk into the completed project.

Companies (and the vendors supporting them) should be very attentive to any disconnect between LOBs and the security organization. Helped by senior management, LOBs and security must meet early in the process to ensure new innovation projects include all of the appropriate IT stakeholders prior to the new product, project or process being fully developed.

Importance Of Creating An Innovation Environment

As many companies feel innovation is a critical component to surviving in this hyper-competitive world in which they do business, it is not surprising that 83% of companies give innovation an importance of 4 or 5 on a 5 point scale. What is surprising are the companies who indicate that creating or fostering such an environment is neutral or even not important for them.

The business line respondents weigh the importance of innovation slightly higher than security/IT respondents – however both groups still clearly put significant emphasis on the importance of innovation overall (Table 4).

TABLE 4

Importance of Creating an Innovation Environment

	Business line respondents:	Security/IT respondents:
Extremely important/important	86.90%	78.00%
Neutral	9.60%	14.40%
Not very/not at all important	3.50%	7.40%

n=197

Source: IDC, 2008

Respondents that believe security has a positive effect on innovation also strongly believe in the importance of innovation, see Table 5 below. Meanwhile the majority respondents who felt that security has a negative or neutral affect on innovation still indicate that innovation is quite important to their firms. This could potentially indicate an opportunity for a savvy vendor to assist these companies in better engaging their security organizations in the development and support of innovative projects and processes in the company. This work could help to reverse the negative views some stakeholders have about interacting with security organizations.

TABLE 5

Security Effect On Business Innovation

	Positive:	Negative:	Neutral:
Extremely important/important	91.20%	70.70%	76.70%
Neutral	7.20%	18.40%	15.70%
Not very/not at all important	1.50%	10.90%	7.60%

n=197

Source: IDC, 2008

When respondents were queried about where the primary responsibility for driving innovation sits within their organizations, IDC did not find any significant swings based on a particular group of respondents (Table 6). Overall, the respondents when grouped by title are fairly balanced in how they rate and rank the importance of innovation. Not surprisingly, executive leadership and the LOBs show a very strong belief in the importance of innovation. We believe a successful innovation process needs to ensure that C-level, technology stakeholders, and LOBs communicate early and often because they are all in the path of the innovation process.

TABLE 6

Security Effect On Business Innovation by Title

	CEO:	BOD:	Exec Lead:	LOB:
Extremely important/important	91.50%	86.10%	80.70%	80.50%
Neutral	8.50%	9.00%	13.00%	16.30%
Not very/not at all important	0%	4.90%	6.30%	3.20%

n=197

Source: IDC, 2008

Importance of an Information Security Leadership Function that can Enable and Impact C-Level Business Priorities

Almost all respondents agreed information security should be part of the innovation process, but as shown later on in this document, good intentions often fail to get implemented. Table 7 below illustrates the respondents' opinions.

An interesting data point to note is that respondents in the \$5–20B in revenues segment do not believe it is important to have information security leaders in a position to influence C-level business priorities. Unexpected data points such as this illustrate there are still a significant number of organizations that have difficulty reconciling business innovation with the need for effective security. IDC believes this issue may manifest most often where free-form innovation processes that are very loosely structured run into highly-structured security processes. Innovation and process don't always mix very well, especially when the rules for innovation are set at the LOB level, and senior management has little oversight.

Security vendors have the opportunity to help these companies identify ways to better integrate their security teams into their business innovation projects. While the other respondents certainly indicate their belief in the importance of information security's participation in the innovation process, this belief does not always correlate with the effective execution of the same.

TABLE 7

Importance of Having Leaders in the Information Security Function Who Can Enable and Impact C-Level Business Priorities

	\$.5 - .9B:	\$1 – 4.9B:	\$5 – 20B:	Over \$20B:
Extremely important/important	81.80%	81.90%	81.10%	87.10%
Neutral	14.50%	15.50%	7.80%	8.80%
Not very/not at all important	3.70%	2.60%	11.10%	4.10%

n=197

Source: IDC, 2008

When asked how important it was for security leaders to influence C-level decisions, the respondents who believed security negatively impacted innovation were not enthusiastic about the interaction (see Table 8).

TABLE 8

Importance of Having Security Leaders Influence C Level Decisions

	Positive:	Negative:	Neutral:
Extremely important/important	92.90%	52.90%	73.10%
Neutral	7.10%	31.60%	17.10%
Not very/not at all important	0%	11.60%	7.20%

n=197

Source: IDC, 2008

Also the line of business respondents only slightly edge out the security/IT respondents in terms of believing information security leadership should have influence on the C-level decision making (Table 9).

TABLE 9

Responses by Function

	Sec/IT:	LOB:
Extremely important/important	74.40%	79.60%
Neutral	15.70%	15.50%
Not very/not at all important	8.40%	1.50%

n=197

Source: IDC, 2008

For respondents indicating C-level/BOD titles have primary responsibility for innovation in their companies, they also believe having security leadership influence C-level decisions is important. Respondents indicating that executive leadership and LOB have primary responsibility for innovation also support the inclusion of security, but less enthusiastically so. Vendors should pay close attention to where the best interests of the stakeholders involved in innovative projects lie. If there is tension between the business line and the information security team, then a vendor should take care to approach the situation in a way that best support the goals of all involved stakeholders (Table 10).

TABLE 10

C Level BOD Level Responses

	CEO:	BOD:	Exec Lead:	LOB:
Extremely important/important	87.60%	81.10%	74.80%	71.40%
Neutral	12.40%	12.60%	19.30%	16.30%
Not very/not at all important	0%	4.90%	3.80%	6.50%

n=197

Source: IDC, 2008

Even though the indication of security's importance is quite positive, respondents may not execute on their desires for integration and influence across organizations. The relationship between the LOBs creating innovative projects, IT maintaining discipline over security processes, and senior management watching top-line business development is poorly synchronized. This is exacerbated by the distant relationships all these parties have with one another.

Top Five Barriers to Innovation

The barriers mentioned above are conventional wisdom, but they provide some guidance for prioritizing solutions. Vendors who are sensitive to the different perspectives of all the stakeholders (e.g., senior management, LOBs, and IT) in a company's innovation process will be better prepared to assist that company with its new product and service development.

When we looked at these results by respondent's title, 51% of respondents who believe the CEO has primary responsibility for driving innovation rated "Information security is not aligned with business goals" as the greatest barrier. IDC believes CEOs are tired of complaints about budgets and resources. They want security to work with business units on appropriate goals for innovation and risk management within the available budget and resources. It will take C-level influence in many cases to encourage the business lines to work with information security as many of the business units feel that information security is still more of a barrier, or at the very least an inhibitor or hurdle, that must be overcome in order for them to realize their vision of innovation.

Top Five Barriers by:

Respondents Who Indicated CEOs Hold Responsibility for Driving Innovation:

- Information security not aligned with business goals (51%)
- Information security turnaround time on business needs too long (31.6%)
- Exec leadership too conservative on information risk (30.3%)
- Limited budget/resources for innovation investments (30%)
- Information security approach too much of a lock down vs. enabling (28.3%)

Respondents who indicated that the BOD holds responsibility for driving innovation:

- Limited budget/resources for innovation investments (45%)
- Information security turnaround time on business needs too long (44.7%)
- Innovation strategy too disjointed/not unified (43.6%)
- Information security not aligned with business goals (36.7%)
- Exec leadership too conservative on information risk (24.1%)

Respondents who indicated that the Exec Leadership holds responsibility for driving innovation:

- Limited budget/resources for innovation investments (46.4%)
- Innovation strategy too disjointed/not unified (38.5%)
- Exec leadership too conservative on information risk (36.5%)

- Business leadership not educated on new/existing security tech (28.2%)
- Information security not aligned with business goals (28.0%)
- Respondents who indicated that the Business unit/LOB holds responsibility for driving innovation:
 - Limited budget/resources for innovation investments (47.6%)
 - Innovation strategy too disjointed/not unified (45.2%)
 - Exec leadership too conservative on information risk (35.5%)
 - Information security turnaround time on business needs too long (23.1%)
 - Information security not aligned with business goals (21.9%)

Measuring Information Security Leadership on Business Growth and Innovation

The results of IDC's survey indicate most companies measure information security on its contribution to innovation. When the top two "Yes" responses are combined, the largest companies seem more aggressive, but mid-tier companies also take this issue seriously. As for responses indicating "No performance measurement", the \$500-999M companies seem to be most the recalcitrant. Still, the fact that over a quarter of respondents' companies take "no performance measurement" action across the board indicates there is a lot of room for misunderstanding and miscommunication about when exactly the security organization should join the development of new innovation.

In addition to ensuring the security organization's success with business goals and innovation is measured, it should not be overlooked that a similar measurement requirement should be made of the business organization. It will do little good to require the security organization to respond to the business requirements if the business lines have no similar responsibility to bring the security team into their planning process when it is most efficient to do so.

As if cementing the validation of the need for performance-based measurement to be driven from above, 86.7% of respondents who indicated that the responsibility for driving innovation lay with the CEO also said their companies have either formal or informal performance measurement requirements on the security leadership to support business growth and innovation as opposed to only 53.6% of respondents who said that the LOB has primary responsibility for driving the innovation in the organization (Table 11).

TABLE 11

Primary Responsibility for Driving Business Innovation

	CEO:	BOD:	Exec Lead:	LOB:
Yes, formal or informal	86.70%	76.30%	65.30%	53.60%
No, performance not tied to innovation	10.10%	22.40%	28.00%	36.60%
Don't know	3.30%	1.40%	6.70%	10.90%

n=197

Source: IDC, 2008

Also not surprising is the split of respondents by their opinion of the impact on security on innovation. For instance, only 50.4% of respondents with a negative impression of security's impact on innovation report the existence of performance metrics for security leadership's contribution to the business goals and innovation of the company. 42.3% of those same respondents report that there are no performance metrics in place, while only 3.2% of those respondents that have a positive impression of the impact security has on innovation report no performance metrics in place. 93.7% of respondents who report a positive impression of security's impact on innovation indicate they have either formal or informal performance plans in place for security leadership's contribution to business goals and innovation (Table 12).

TABLE 12

Innovation Tied to Performance

	Positive:	Negative:	Neutral:
Yes, formal or informal	93.70%	50.40%	45.40%
No, performance not tied to innovation	3.20%	42.30%	43.90%
Don't know	3.10%	7.30%	10.70%

n=197

Source: IDC, 2008

It is very clear that companies driving innovation through performance requirements have a much better chance of ensuring information security has a positive influence on their organization's business goals and bottom line. The top business innovation initiatives respondents' companies are pursuing and/or have been funded over the next 18-24 months are:

- ☒ New joint ventures (50.6%)
- ☒ Enhanced business performance measurement (46.9%)
- ☒ Enhanced governance, risk and compliance (42.9)
- ☒ Supply chain innovation (42.4%)
- ☒ Customer self-service models (40.9%)

Off-shoring is next to the last (and thus not represented above), and it is not surprising that companies don't consider off-shoring to be very innovative. Even lower on the list of innovative initiatives is Web-based collaboration. IDC believes the lack of familiarity with Web 2.0 technologies as well as the belief that these new tools are just for "kids to gossip with one another," (according to anecdotal comments that IDC has heard from senior management, IT, and business units leaders) drives down the demand for using such tools in an innovative manner. While these comments did not come out of the survey, enterprises often voice fears that most Web 2.0 applications lack good security.

And while off-shoring and Web collaboration are low on the list of priorities, 29% and 28% of respondents respectively indicate they are either pursuing and/or have funding for projects of these types in the next 18-24 months.

The type of innovative initiatives being funded or considered for funding over the next 18-24 months is split by respondent's role, either Security/IT or LOB, and the top five initiatives for each are as follows (see Table 13):

TABLE 13	
Security/IT or LOB the Top Five Initiatives Over Next 18 to 24 Months	
Security/IT:	LOB:
Supply chain innovation (48.8%)	New joint ventures (54.5%)
Enhanced business performance measurements (47.2%)	Enhanced business performance measurements (46.7%)
New joint ventures (46.5%)	Enhanced GRC mgmt (44.4%)
Collaboration w/ external partners (43.4%)	Mergers/acquisitions (40.0%)
Customer self-service models (42.3%)	Customer self-service models (39.5%)

TABLE 13**Security/IT or LOB the Top Five Initiatives Over Next 18 to 24 Months**

Security/IT:

LOB:

n=197

Source: IDC, 2008

Types of Innovative Initiatives Pursued and/or Funded Over the Next 18 to 24 Months by Company Revenue

Interestingly, the top three initiatives of respondents when segmented by company revenue are:

- Over \$20B:
 - New joint ventures (53.2%)
 - Global sourcing (46.5%)
 - Customer self-service models (45.9%)
- \$5 – 20B:
 - New joint ventures (57.0%)
 - Enhance business performance measurements (55.0%)
 - Global sourcing (46.1%)
- \$1 – 4.9B:
 - Mergers/acquisitions (45.9%)
 - Enhanced business performance measurements (45.6%)
 - New joint ventures (43.4%)
- \$500 - 999M:
 - Enhanced governance, risk and compliance management (56.0%)
 - New joint ventures (51.4%)
 - Supply chain innovation (46.0%)

The smaller companies obviously have more concerns about keeping up with new governance, risk and compliance concerns, but all are interested in utilizing joint ventures as a way to increase innovation and share risk with other firms who may have very similar goals and complimentary skills and resources.

In general the priorities hold true regardless of the company size, with the exception of the \$500-999M segment. This segment seems to be belatedly coming to the realization that they must do something about the efficiency of the governance

process. IDC believes joint ventures enable innovation while lowering risk through because the development is shared with another organization.

The data also shows the initiatives in which the least amount of respondents indicated investment. For instance, the \$500-999M revenue segment has very little investment in business process off-shoring (12.7%), followed closely by the \$1–4.9B revenue segment's very low interest in web-based collaboration. It is only when a company reaches a very large size does it start to find that information management can be quite innovative – hence the interest of companies with over \$20B in revenues having interest in web collaborative tools (37.4%).

Additionally, looking at each of the initiatives reveals the revenue "sweet spots" for that initiative based on respondents' answers. For instance, 55% of respondents from \$5—20B companies indicate enhanced business performance measurements are an initiative in the next 18-24 months.

Rating the Effectiveness of Respondents' Organizations at Assessing the Information Risk Associated with Potential Innovation

All respondents are highly confident of their risk assessment capabilities, but only approximately 20% rate themselves as extremely effective. In other words, they see room for improvement. However, IDC believes business priorities may outweigh risk in some cases so some companies never intend to get to the extremely effective level because it is simply not a profitable goal. In other words, they are not willing to spend 80% to get that last 20% of improvement.

Responses also seem to indicate that once a company has reached around the 60% level of effectiveness, it is then a slow climb to a short distance away. At least as indicated in this survey, the respondents don't seem to progress much past the low 60's in terms of effective risk assessment of potential innovation (Table 14). The biggest variations going forward seem to live in moving the company past the stage of being not effective to either neutral or effective with regards to assessing the risk associated with innovation.

TABLE 14

Assessing Risk Of Potential Innovation				
	\$.5 - .9B:	\$1 – 4.9B:	\$5 – 20B:	Over \$20B:
Extremely effective/effective	53.60%	61.90%	62.10%	64.20%
Neutral	17.90%	29.50%	23.60%	29.50%
Not very/not at all effective	21.50%	8.10%	14.30%	1.10%

n=197
Source: IDC, 2008

It is also interesting to note how significantly opinions of risk assessment effectiveness differ depending on whether or not the respondent has a positive or negative impression of security's impact on innovation. Clearly, those respondents with a positive impression of security's impact on innovation also believe their organization is very effective at assessing the risk associated with potential innovation. While this has many possible implications, we believe there is a correlation between the involvement of security at the highest level and a confident approach to risk assessment (Table 15).

TABLE 15

Effectiveness Based on Opinion

	Positive:	Negative:	Neutral:
Extremely effective/effective	84.90%	40.00%	41.70%
Neutral	13.10%	29.40%	42.10%
Not very/not at all effective	0.40%	23.30%	15.60%

n=197

Source: IDC, 2008

Assertive, Compliant or Fearful Organization Descriptions

Compliance, not fears or threats, are driving security strategies. This is no surprise because compliance poses the greatest risk to innovation. How do people collaborate so they can receive the most information possible, but corporate and customer privacy is enforced? A company needs strong federated authorization and authentication, along with the ability to correlate and analyze possible violations before they occur. The lines of business must work with the security organization in order to best understand what is driving the requirements of each organization and how to most effectively implement those solutions (see Table 16).

TABLE 16

Issues Driving Security Strategies

	\$.5 - .9B:	\$1 – 4.9B:	\$5 – 20B:	Over \$20B:
Fear/threat driven	17.80%	12.60%	17.40%	18.90%
Compliance/control driven	67.40%	66.20%	53.20%	57.30%
Business acceleration driven/confident	13.90%	18.10%	29.40%	18.50%

TABLE 16**Issues Driving Security Strategies**

	\$.5 - .9B:	\$1 – 4.9B:	\$5 – 20B:	Over \$20B:
Don't know	1.00%	3.10%	0%	5.20%

n=197

Source: IDC, 2008

A larger percentage of respondents with negative impressions of security report their companies are compliance and control driven. IDC believes organizations without an appreciation for security will struggle with compliance governance issues.

Respondents with a positive impression of security were more confident and focused on business growth and acceleration, although the majority of them do indicate they are also compliance/control driven. The reality of the situation is that even if the company is motivated by compliance and controls, IDC believes that if the relationship between security and innovation is managed correctly and driven from the C-level in the organization, then the rest of the organization will fall into line.

If a vendor knows their target company is business acceleration driven and confident, then it is more likely to succeed at meeting both the security requirements to protect their business and the innovation requirements to make it grow. This combination will make the company an attractive customer from which any vendor should court a relationship.

TABLE 17**Impressions Of Security**

	Positive:	Negative:	Neutral:
Fear/threat driven	16.20%	16.40%	17.30%
Compliance/control driven	52.30%	73.50%	65.60%
Business acceleration driven/confident	29.90%	9.10%	13.80%
Don't know	1.60%	1.00%	3.20%

n=197

Source: IDC, 2008

Frequency of Organizational Shying Away from Innovative Business Initiatives Because of Potential Information Risks

For the whole survey population, enterprises admit to backing away from innovation with potential information risk over half the time. In fact, more than 80 percent of the executives surveyed admitted that their organizations have chosen not to pursue innovative business opportunities because of information security concerns.

At the lower-end of the survey's respondents (\$500-\$999M in annual revenues), this figure rises to almost three quarters indicating the much more conservative nature of the smaller organizations.

The data below are fairly inconclusive with regards to any particular trends other than as a company grows larger, it does seem to become less risk adverse and less willing to back away due to risk in innovation. However, this observation is skewed a little by the large percentage of Over \$20B respondents who indicated "Don't know." The data indicates the most risk-tolerant revenue segments are the \$5–20B respondents, with the Over \$20B segment starting to gain back a little more risk aversion.

TABLE 18

Shying Away from Innovative Business Initiatives Due to Information Risks				
	\$.5 - .9B:	\$1 – 4.9B:	\$5 – 20B:	Over \$20B:
Often	12.50%	21.40%	35.30%	21.90%
Occasionally	71.40%	61.70%	48.10%	51.90%
Never	9.20%	11.70%	10.40%	7.30%
Don't know	7.00%	5.10%	6.20%	18.90%

n=197
Source: IDC, 2008

About 35% of respondents who are positive about security's impact on innovation report their companies often back away from innovation due to potential information risks, while only 16.3% of those who report a negative impression of security indicate their companies often back away from innovation. IDC believes larger companies with better developed security policies are better at assessing the risks of collaboration. Therefore, they are somewhat more cautious. Companies with a lower regard for security don't know or care about the risks of collaboration and innovation, and so they are willing to take much greater chances. In other words, ignorance is bliss.

TABLE 19**Impressions Of Shying Away from Innovations Because of Information Risks**

	Positive:	Negative:	Neutral:
Often	35.50%	16.20%	14.40%
Occasionally	40.60%	78.10%	68.40%
Never	17.20%	4.80%	4.40%
Don't know	6.70%	1.00%	12.80%

n=197

Source: IDC, 2008

Potential Consequences of Excluding Information Security in the Innovation Process

Why is security stifling innovation? The biggest issue identified by respondents is the fact that security is stifled by budgetary constraints. The second reason cited was misplaced priorities. Even Security/IT people agree that confusion over perceived vs. real threats is stifling innovation.

Top three potential consequences associated with excluding information security in the innovation process:

- An innovative project fails because of poor information access
- Information security risks associated with innovative initiatives are too high because security was not brought into the process
- Ultimately slower time to market and higher costs when security needs to be bolted on as an afterthought.

Very large companies are mostly concerned with fraud as a consequence of not bringing security in early enough as well as privacy/security breaches. Overall, the trends are consistent across the revenue segments. The priorities are really about ensuring that projects don't fail, risks are addressed appropriately and the new product or service gets to the market in a timely enough manner to ensure a competitive edge.

- Over \$20B
 - Potential fraud (52.6%)
 - Information security risks associated with innovative initiatives are too high because security was not brought into the process (50.2%)

- Privacy or security breaches (48.5%)
- \$5 – 20B
 - An innovative project fails because of poor information access (72.8%)
 - Information security risks associated with innovative initiatives are too high because security was not brought into the process (64.3%)
 - Ultimately slower time to market and higher costs when security needs to be bolted on as an after thought (62.9%)
- \$1 – 4.9B
 - Ultimately slower time to market and higher costs when security needs to be bolted on as an after thought (67.8%)
 - Information security risks associated with innovative initiatives are too high because security was not brought into the process (64.6%)
 - An innovative project fails because of poor information access (62.4%)
- \$.5 - .9B
 - Information security risks associated with innovative initiatives are too high because security was not brought into the process (46.6%)
 - Ultimately slower time to market and higher costs when security needs to be bolted on as an after thought (46.6%)
 - Privacy or security breaches (45.2%)

Reflecting the consistency is the difference, or rather the lack of difference, in the priorities of the Security/IT respondents versus the LOB respondents. Each group of respondents indicates the exact same top three potential consequences, practically down to the percentages as well. The only slight differences are the order in which they are prioritized.

- Security/IT
 - Information security risks associated with innovative initiatives are too high because security was not brought into the process (61.4%)
 - An innovative project fails because of poor information access (56.2%)
 - Ultimately slower time to market and higher costs when security needs to be bolted on as an after thought (55.6%)
- LOB
 - An innovative project fails because of poor information access (62.2%)
 - Ultimately slower time to market and higher costs when security needs to be bolted on as an after thought (60.4%)

- ❑ Information security risks associated with innovative initiatives are too high because security was not brought into the process (55.6%)

Information Security Team Engaged in Business Innovation Initiatives

The data indicates the respondents have good intentions about security's inclusion into innovation projects, but execution of the same seems poor (Table 20).

The smaller the company, the less likely it is to involve information security early in business innovation initiatives. Their intentions may be good, but it is highly likely that a smaller company has fewer compliance and governance requirements and therefore, the business innovators do not involve the information security people until it is absolutely necessary. Clearly the larger the company, the more likely it is that it will have strict guidelines on when information security should be engaged by the project team. In the case of this particular survey, the over \$20B group has a significant percentage of financial services organizations that are highly regulated for privacy and information security and therefore, this awareness and institutional rigor is reflected in the data.

TABLE 20

When Is Information Security Engaged In Business Innovation Initiatives?

	\$.5 - .9B	\$1 – 4.9B	\$5 – 20B	Over \$20B
Early in planning	25.70%	34.50%	26.30%	39.50%
Plan review/sign off	26.90%	31.90%	38.40%	29.40%
At launch	16.00%	14.60%	16.40%	1.10%
After launch	14.30%	3.80%	4.40%	7.00%
Reactionary	9.20%	4.00%	9.30%	3.90%
Not at all	1.00%	6.60%	2.40%	0%
Don't know	7.00%	4.60%	2.40%	19.10%

n=197

Source: IDC, 2008

The respondents who have a negative opinion of security's influence on innovation very clearly do not involve the organization until they absolutely have to, with almost 11% of this segment not engaging the information security organization at all – in comparison to 0% and 1.1% as reported by the positive and neutral segments respectively. Also 42% of respondents reporting a positive impression of security's influence also indicate they bring in information security early in the planning there is

a significant difference when compared with the neutral segment's 30.9% and the negative segment's 12.6%.

TABLE 21

Opinions of When Security Should be Brought in on Business Innovations

	Positive:	Negative:	Neutral:
Early in planning	42.00%	12.60%	30.90%
Plan review/sign off	33.40%	38.20%	29.90%
At launch	16.60%	7.50%	10.70%
After launch	4.40%	6.50%	10.40%
Reactionary	2.00%	12.60%	7.40%
Not at all	0%	10.70%	1.10%
Don't know	1.60%	11.90%	9.50%

n=197

Source: IDC, 2008

There is little difference between what the respondents see when split by functions within the organization – the most obvious perhaps being that 16.7% of Security/IT respondents report bringing information security in at launch while only 9.6% of LOB respondents report bringing in information security at launch (Table 22).

TABLE 22

LOB and Security/IT Opinions of when security should be brought in on business innovations

	Security/IT:	LOB:
Early in planning	30.60%	32.00%
Plan review/sign off	35.90%	29.00%
At launch	16.70%	9.60%
After launch	3.40%	9.60%
Reactionary	5.40%	7.50%
Not at all	2.80%	3.40%

TABLE 22

LOB and Security/IT Opinions of when security should be brought in on business innovations

	Security/IT:	LOB:
Don't know	5.10%	8.80%

n=197

Source: IDC, 2008

Information Security Function's Impact on Innovation Process

In all cases, Moderate Positive Impact is the prevailing view. No and Negative Impact are the greatest for the \$500-999M because these companies move quicker than their larger counterparts and are more highly sensitive to any obstruction to innovation and growth.

Respondents who report their physical and information security is not yet consolidated report a much higher negative impact of information security function on the innovation process than those respondents that have consolidated those two functions. Those that have not consolidated the functions also report much lower significant positive impact. However respondents from both segments report about similar levels of moderate positive impact.

TABLE 23

Information security function impact on the innovation process

	Consolidated:	Not consolidated:
Physical & Information Security	34.90%	8.30%
Significant positive impact	48.60%	41.70%
Moderate positive impact	8.30%	28.30%
Negative impact	3.70%	18.30%
No impact	4.50%	3.30%

Don't know

n=197

Source: IDC, 2008

Reporting Structure of Most Senior Information Security Individual

Overall, information security reports into the IT organization, but there is a growing trend towards the function reporting into the CEO. However, for the mid-tier and very large organizations, there is an almost equal distribution of reporting to the CEO as well as the IT organization. For the mid-tier organizations, it most likely has to do with the smaller executive staff organization allowing for information security to be much closer to the C-level executives. However, very large organization indicates that proximity to the CEO is due to the increasing priority of the information security function as the company moves up the scale in size, scope and complexity. Information security will become an increasingly critical function the larger the organization is, and it will need to ensure that the function has the appropriate levels of access to executive management for raising business-critical issues.

Over half of the respondents who indicated the primary responsibility for driving innovation lies with the CEO also report that the information security function reports to the CEO. In the case of the BOD having responsibility for driving innovation, almost half of those respondents indicated that information security reports into the IT (CIO) organization. For those respondents who indicate the line of business as having responsibility for driving innovation, the information security group reports into many more locations in the organization including into finance and risk/compliance office.

TABLE 24

Most Senior Security Staff Reporting

	CEO	BOD	Exec Lead	LOB
CEO	51.30%	22.20%	18.10%	10.40%
IT (CIO)	37.70%	49.30%	44.10%	53.20%
Operations (COO)	5.90%	2.70%	17.70%	7.60%
Finance (CFO)	4.10%	9.00%	5.10%	10.00%
Risk (CRO)	0%	6.60%	9.00%	13.70%
Legal (Gen Counsel)	0%	0%	4.00%	2.50%
BOD/Board Committee	0.90%	10.20%	0%	0%
Other	0%	0%	2.00%	2.50%

n=197
Source: IDC, 2008

When asked to whom the senior security person should report, respondents seemed to agree that IT security reporting structures were fine, even security/IT respondents

felt they should report to the CIO. However, a few respondents indicated information security should report to organizations such operations or risk, where the information security organization might have a greater opportunity to be integrated in to new project innovations that are being generated. Among the largest companies, however, IT security should report directly to the CEO.

TABLE 25

Who Should the Most Senior Security Staff Report to?

	To Whom Does Infosec Report?	To Whom Should Infosec Report?
CEO	23.70%	25.40%
IT (CIO)	45.70%	37.60%
Operations (COO)	10.00%	13.80%
Finance (CFO)	6.60%	5.90%
Risk (CRO)	7.90%	10.30%
Legal (Gen Counsel)	2.80%	2.30%
BOD/Board Committee	2.00%	3.30%
Other	1.40%	1.40%

n=197

Source: IDC, 2008

Board Level Importance of Information Security

Regardless of company size, effectively two thirds of all respondents feel information security is a board-level issue. This opinion also breaks out pretty evenly when respondents are divided by of either Security/IT or LOB – with over two thirds of each segment in agreement of the importance of information security. Even a third of the respondents who believed that information security had a negative impact on innovation still indicated information security should be an important board level issue (Table 26).

It is clear that information security continues to rise in importance. The biggest challenge is how organizations will integrate their information security functions into their business. The impact of not paying attention to the security of a company's information has enormous consequences for all the stakeholders in the business. IDC believes that while everyone agrees on the importance of security, they still do not want it interfering with their projects.

Selling Information Security to Executive Leadership

Information security is still a fear-based sell that focuses on compliance, reputation threats, internal/external threats, and failed audits (tying back to compliance). While the "sales pitch" may still be fear based, the reality is as companies get more competent at assessing their risk, they become more aware of why a strategic security approach is critical to business growth, competitive positioning and brand equity.

TABLE 26

Opinions On Whether Information Security Is a Board-Level Issue

	Positive:	Negative:	Neutral:
Extremely important/important	80.30%	36.70%	54.50%
Neutral	13.50%	35.00%	26.00%
Not very/not at all important	3.10%	28.30%	17.20%

n=197

Source: IDC, 2008

IDC's survey shows very little variation across respondents' answers with regards to how information security is sold to executive management – currently and for the foreseeable future – it remains fear based.

As the transparency of information increases, so the regulations controlling what companies can and cannot do with the information they create and obtain gain in complexity. The amount of time, effort and funds companies must spend on keeping up with the regulations is significant. By integrating information security into the business innovation process at an early point – as a business enabler or competitive positioning – managing the "fear-based" concerns will be proactive instead of reactive. This in turn should go a long way to helping the organization stay proactive to address and manage risk at a level they are most comfortable.

Successful Strategies in Getting Information Security Involved with Innovation

IDC asked respondents to rank the strategies they believe will be most successful in getting information security involved with innovation. As the results of this question are mean scores on a scale of one to five with one being the highest, the lowest cores have the highest importance.

- Ensure the security organization understands the industry and the business goals of the organization (1.4).
- Ensure enabling business innovation is part of the charter or on the scorecard for measuring the information security function (1.4).

- ☒ Communicate a well-defined roadmap for security that ties to corporate strategy and share it with other business functions (1.6).
- ☒ Ensure the security organization has connections with key business leadership (2.0).
- ☒ Demonstrate how security technology investments have direct links to business priorities (2.0).

All five of these strategies relate to ensuring the information security organization not only understands the business goals of the organization, but also has access to the right leadership members in the organization as well as has a well-defined roadmap and performance metrics plan to ensure they stay in line with the business goals of the organization.

The respondents are pretty much in agreement regardless of their revenue size and segment as to the most important strategies. The only real variation is with the small companies of \$500-999M – as they don't rate "Ensuring that enabling business innovation is part of the charter or scorecard..." as the number two strategy – rather they believe that "Communicate a well-defined roadmap for security..." is slightly more important.

The real take away from this data is the respondents' collective agreement on what is important. No matter which way this data is viewed there is an overwhelming similarity in the priorities. A vendor may then find ways to help these organizations meet their goals by finding ways to enable information security to become more involved, earlier on, with new innovation projects, products and services.

What Can Vendors Do?

IDC asked respondents what vendors can do to help companies integrate information security into innovation project, products and services. Respondents' responses were ranked on a scale of 1 to 5, where 1 is the top rank. The top five responses are:

- ☒ Understanding the organization is the top way that vendors can help companies integrate information security into innovation (2.2)
- ☒ Understanding the client's specific vertical industry and its particular direction, challenges and priorities (2.6)
- ☒ Having a solid understanding of customer, partner and employee collaboration needs (2.8)
- ☒ Showing how security technologies align to specific business priorities (2.8)
- ☒ Providing risk assessment services (2.9)

There are of course a few variations based on the size of the company, but even still those variations are quite minor and the marching orders for the vendors based on what their customers want is pretty clear. For instance, small companies of \$500-999M place more importance on vendors "Offering integrated solutions versus point

products" than they do on vendors "Showing how security technologies align to specific business priorities." Beyond that one particular variation, most of the differences lie in slightly different levels of importance being placed on particular traits.

The message from this data appears to be that respondents really know what they want from their vendors, and it is now the vendors' opportunity to fulfill the needs the respondents have illustrated so clearly.

Services Above and Beyond Day to Day Activities Provided by the Information Security Organization

When asked about the services beyond day to day operational activities the information security organization is being asked to do or improve upon, respondents listed the following top five services:

- Quicker turn around time on providing user access (41.3%)
- Quicker turn around time on risk reviews (40.8%)
- Provide ways to make it easier for customer to access information (36.3%)
- Make more information available to customers (34.9%)
- Establish methods to increase customer loyalty (32.0%)

Top three for respondents segmented by revenues:

- Over \$20B
 - Quicker turn around on risk reviews (48.3%)
 - Provide ways to make it easier for customer to access information (47.5%)
 - Make more information available to customers (43.4%)
- \$5 – 20B
 - Quicker turn around on providing user access (46.9%)
 - Quicker turn around on risk reviews (43.7%)
 - Less restrictive controls at the end user point (39.3%)
- \$1 – 4.9B
 - Quicker turn around on providing user access (43.2%)
 - Quicker turn around on risk reviews (36.6%)
 - Provide ways to make it easier for customers to access information (35.0%)
- \$.5 - .9B

- Less restrictive controls at the end user point (39.8%)
- Quicker turn around on risk reviews (37.1%)
- Establish methods to increase customer loyalty (34.7%)

In general, the respondents are pretty close to one another in what the information security group is being asked to do that is not part of day to day operations of the organization. There are a few variations on theme, but the trends of "efficiency in turn around times" and "easier access to more information for customers" are clear messages coming through this data. IDC believes these elements are critical to collaboration needed for innovation. Quickly provisioning access is crucial to getting a quick start on innovation projects while controlling risk from inappropriate access.

Key Findings In Verbatim Questions

Verbatim Question 1: Define 'business innovation' in your market or organization.

- "A better way of performing a process."
- "A proactive step a business takes to make themselves or their product or even how they internally do business, better than the competition."
- "Business innovation is about adopting new and better technologies to stay ahead of the competition in terms of offering better products and faster services."
- "Business innovation is when a business starts using techniques that are novel and unique, in order to better serve its customers and/or employees. It typically increases worker productivity."
- "Development of methods to reduce costs or increase revenues (what else?)."
- "I define it as something which is fundamentally unique and improves business on day to day basis."
- "New idea or vision the help the organization to excel in the market place compare to other organization."
- "In economics, business and government policy - something new - must be substantially different, not an insignificant change. In economics the change must increase value, customer value, or producer value."
- New products and processes to accomplish core business drivers, expand existing lines, delivery of products/services, and new channels to market."
- "We are in a constant state of flux, attempting to change with the markets and yet offer a service distinct from our competitors."

Verbatim Question 2: What things is the information security team at your organization doing to enable innovation?

- "1. Business model innovation 2. Changing the way the organization is run to achieve competitive differentiation (customer-centric, creating new value) 3. Collaboration 4. Creating an environment and infrastructure that encourage knowledge and information dissemination."
- "Blocking us at every turn with over zealous security practices. In other words, they do not help at all. Totally useless."
- "Breaking down barriers, while maintaining security."
- "Consolidating controls and implementing more automated security options."
- "Decentralizing developers so that they can become embedded in business lines."
- "Don't see the relation of information security to enabling innovation."
- "Enabling business to try out new strategies without risking security, collaborative working with partners, and more secure access for partners."
- "Improving access to sales information, patient records, uptime, mobility, wireless, and other new technologies."
- "Keeping ahead or at least up to date with new & perspective threats, keeping our business secure and protecting our investments."
- "Pursuing de-perimeterization and consumerization strategies using risk methods to select the right security levels taking a data-centric approach to the implementation of security protection, as opposed to infrastructure-centric."
- "Reviewing whole business process."

Verbatim Question 3: Please share any additional comments or thoughts you might have on security's impact on business innovation.

Based on the verbatim comments, the 17 positive comments highlighted security's ability to benefit the business, not just protect it. The 14 negative statements saw security as an impediment to business operations.

Respondents with positive comments said:

- "Give leadership the freedom to lead."
- "Enables higher business growth and drives revenues."
- "If involved at the early stages of planning, security can have a positive impact by making business innovation less risky."
- "Having good security affects business innovation."

- "Innovate or die... We need to be in front with new ideas to succeed."
- "I know in my organization, if information security is aligned with business innovation, the sky is our limit. Thanks and god bless."
- Respondents with negative comments said:
- "In general security stifles business innovation."
- "Governmental regulation is outpacing innovation."
- "It depends which country you live in, but in a globalized world a need for security has become more apparent. Only sometimes it can stifle relationships."
- "It is restrictive!"
- "It slows down innovation. But definitely saves from threats."
- "It's not an enabler - security is something that needs to be built into any innovative work."

Define 'business innovation' in your market or organization? (based on Verbatim Question 1)

- Better/faster ways to beat the competition,
- Creating new and/or improved ideas,
- Creating new products & services for customers.

Vendors can help their customers reach their goals by:

- Understanding the organization and its industry.
- Gaining knowledge of their customers internal and external relationships and identifying the best method of support
- Showing how security technologies align with specific business priorities and helping the customer understand how best to execute on those synergies

CONCLUSION

Business cannot grow without the incubation and support of new innovations. Similarly, because today's companies must use sophisticated computing equipment to stay competitive, the challenges of protecting the business from internal and external threats to those systems continue to escalate. While at first glance it may seem that innovation and security are two competing priorities, IDC believes they are complementary.

The survey conducted by IDC and funded by RSA reviewed how almost 200 top businesses and security executives worldwide thought about the impact of information security on business innovation. It is clear that perspectives and execution against those perspectives varies widely. Yet despite the many different ways to think about and act upon the delivery of both innovation and information security, respondents identified several clear trends:

- ☒ We are still operating in an environment where compliance and fear, rather than the potential business advantages of information security, are driving strategic decisions about security.
- ☒ While approximately 80% of respondents consider themselves effective in assessing their risk, only 20% consider themselves extremely effective.
- ☒ IT Security risk is the single biggest inhibitor to business innovation, with more than 80 percent of the executives surveyed admitting their organizations have occasionally or often backed away from innovative business opportunities because of information security concerns.
- ☒ A delta exists between the desired business alignment of information security and the fear-driven methods of selling the same to upper management.

These findings show a significant opportunity for forward-thinking security leaders and savvy vendors to help businesses better align their information security and business innovation needs. By better understanding of an organization's business, industry, focus and even internal politics, security practitioners and their vendors will be better positioned to support these businesses innovating in a way that does not increase their risk or compromise their need to comply with information security requirements.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2008 IDC. Reproduction without written permission is completely forbidden.