

2010 Energy & Resources
Global Security Study
Continuing the journey



Content

1	Foreword
2	Who responded
3	Key findings
6	Detailed results
7	Governance
14	Information security budget
15	Threat landscape
21	Use of security technologies
23	Business Continuity Management (BCM)
24	Outsourcing and third party security management
26	Privacy
27	Compliance
28	Energy and resources specific questions
30	How the survey was designed, implemented and evaluated
31	Acknowledgements
32	Contacts

Foreword

Welcome to the 2010 Global Security Survey for the Energy & Resources (E&R) industry, based on research, conducted mostly in person, with over 100 E&R organizations.

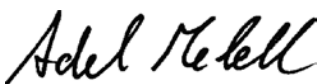
Rather than just report findings, we have attempted to bring the perspective of our experience and to make practical and helpful recommendations where appropriate. We hope you find this study an informative and useful read.

It is anticipated that the E&R industry that powers the world may experience a myriad of changes in the coming months. These changes are likely to compel the industry to revisit the way it protects its data, whether within its walls, in the hands of third parties or in the sky via cloud computing. These changes mean that organizations need to be vigilant about how changes will impact them and should take appropriate actions to continue the journey towards strong information security.

The most significant changes for power & utilities organizations is the continued rise of Smart Grids, which have the potential to revolutionize the power sector by significantly reducing energy consumption by decreasing the need to construct new power plants. However, despite their benefits, the use of Smart Grids multiplies risk factors including threats to the distribution of energy and the privacy of consumers. Protecting the Smart Grids and other industrial components, including the Smart Meters, is important to the success of this venture.

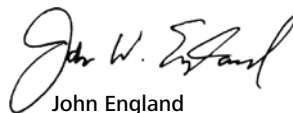
The oil and gas sector is now likely to experience an increase in mergers and acquisition activities as we continue to recover from the recent economic crisis. Targets may include the independent and junior oil organizations that have struggled during the recession. The mergers and acquisitions environment is susceptible to data breaches: the integration of disparate computer systems, cultural differences, differing information security policies and procedures, and differing regulatory requirements.

On behalf of the member firms of Deloitte Touche Tohmatsu Limited (Deloitte¹), and the Energy & Resources practices of its member firms, we would like to thank all the people who contributed to this report and generously shared their experiences and insights.



Adel Melek

Global Managing Director, Information & Technology Risk
Deloitte Touche Tohmatsu Limited



John England

Global Energy & Resources, Enterprise Risk Services
Deloitte Touche Tohmatsu Limited

¹ Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Who responded

In order to promote open and candid discussion, Deloitte has preserved the anonymity of the survey participants. The majority of this study information was collected through face-to-face discussions.

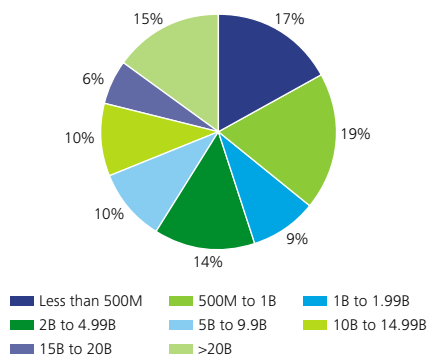
Respondents to the 2010 E&R Security Study range from large organizations, with annual revenues of over \$15 billion to organizations with less than 500 employees.

Among participating organizations, nearly half of respondents report revenue of less than US\$1 billion and greater than US\$20 billion and nearly half employ between 501 and 10,000 employees. Electric and oil & gas organizations are the two biggest sectors represented (40 percent and 32 percent, respectively).

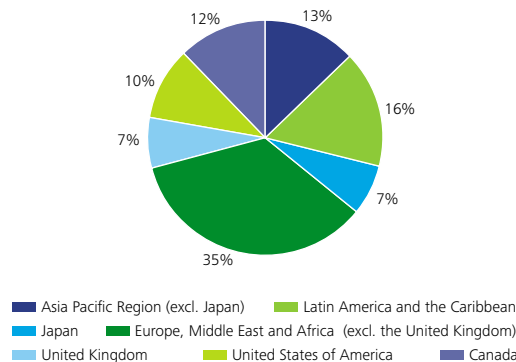
Electric and oil & gas organizations are the two biggest sectors represented (40 percent and 32 percent, respectively).

Geographically, the most well represented region in this year's study is Europe, Middle East and Asia (35 percent of respondents), followed by Latin America and the Caribbean (16 percent), Asia Pacific (13 percent), Canada (12 percent), United States of America (10 percent), United Kingdom (7 percent) and Japan (7 percent).

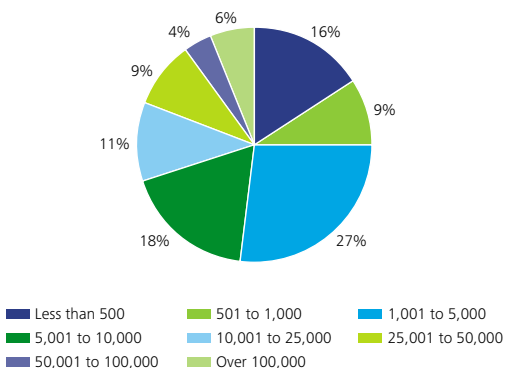
By revenue



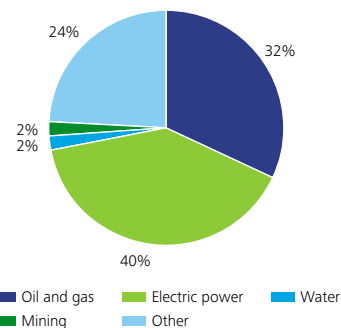
By region



By headcount



By sector



Note: The data included in certain of the charts will not total 100%. Please refer to "How the survey was designed, implemented and evaluated" section for a description of the methodology used to determine the data for inclusion.

Key findings

The role of the information security executive is considered a predominantly IT role

Although the majority of E&R organizations have an executive responsible for information security or a Chief Information Security Officer (CISO), the survey reveals that for a large percentage of organizations, the reporting relationship is predominantly to IT-related positions: CIO, CTO and IT executive.

When information security is perceived by the organization to be mainly an IT-function, it may become more difficult for the function to demonstrate its value to the business. This perception, in turn, can contribute to barriers to information security, such as lack of visibility and influence and lack of support from the lines of business.

It is interesting to note also, from the survey responses, that the CISO's focus appears to be heavily weighted to digital assets, despite evidence that loss of paper-based information (a prevalent form of information storage) and other information in non-digital formats can have significant ramifications to the organization.

Investment in information security is increasing as the economy improves

Overall, lack of sufficient budget is considered by respondents to be less of a barrier to information security this year than last year. Investment in information security is continuing an upward trend although a quarter of respondents have had their budgets reduced. Without continuous investment in security and innovation, organizations that have had their budgets cut may be unlikely to keep pace with the growing threats from increasingly sophisticated attacks and emerging technologies.

Most organizations do not have an executive responsible for privacy nor do they have a program for managing privacy compliance

The E&R industry appears particularly vulnerable to a catastrophic breach of information security and privacy. E&R organizations handle large quantities of distributed sensitive information; their reputations and business success hinge, in part, on safeguarding this information. Most organizations do not have a Chief Privacy Officer; however, as legislation for the industry increases, it is likely that this position will become more common. The greatest percentage of respondents do not have a program for managing privacy compliance nor do they have a formal process to deal with complaints about personal information management practices.

When information security goals and objectives are not aligned with those of the business, respondents tend to cite lack of visibility and lack of executive support for the function

Information security functions continue to grow steadily within the E&R industry. This year, 76 percent of respondents report a headcount of up to 25 full-time security employees, however some respondents report having no full-time security employees. This would indicate that these organizations may not have the basic necessities when it comes to information security. Moreover, the majority of respondents state that their organization is missing skills and competencies to handle existing and foreseeable security requirements. The two most frequently mentioned barriers to ensuring information security are lack of visibility and influence within the organization and lack of support from lines of business. These barriers correlate to the finding that only 22 percent of respondents consider their information security objectives to be "appropriately aligned" with those of the business. Involvement of the business in the information security strategy at the outset and a strategy that takes into account the objectives of both areas is paramount. Only 53 percent of respondents have a documented and approved information security strategy but the good news is that the information security strategy was noted as one of the top information security initiatives for this year.

Respondents recognize the connection between security and privacy breaches and internal people

One of the main concerns of the industry is accidental breaches of information originating from inside the organization. Top threats include “Non-intentional loss of sensitive information” and “Employee errors and omissions”. Respondents plan to counter these threats with information security training and awareness programs – demonstrated to be very effective in changing inadvertent behavior – and information security governance, which helps to establish a data security mindset and culture. Respondents also cite “Increasing sophistication and proliferation of threats” as a top concern which is expected to be tackled by the initiative to improve the security infrastructure. To enhance the infrastructure is important but it is also important to help internal people recognize their role in inadvertently aiding and abetting external criminals through phishing attempts, social networking sites, and mule scams.

Data protection is now a top-five security initiative

Information is most organizations’ lifeblood and protecting it must be a priority. One of the biggest challenges when implementing a data protection program is identifying the data that needs protection. Experience in the field has shown us that many organizations do not know what data they should be protecting.

Although “security infrastructure improvement” is still the top initiative named by survey respondents, data protection and two other new initiatives have moved into the top five:

- Security infrastructure improvement
- Information security governance – Newcomer
- Information security strategy
- Information security training and awareness – Newcomer
- Data protection – Newcomer

Identity & access management, business continuity and information security regulatory and legislative compliance disappeared from the top information security initiatives list. Priorities have shifted dramatically this year and the focus is on improving the infrastructure, creating a robust strategy that deals with setting the overall control framework and training employees.

The results this year indicate that there is very little focus on third party security initiatives. Given that EGR organizations heavily depend on third parties, this lack of focus may well represent a security gap.

Energy & Resources organizations should consider regularly reviewing and testing vendor security capabilities, controls, and organizational dependencies.

The majority of organizations do not track and monitor the effectiveness of their compliance programs

Failure to comply with regulations can expose an organization to hefty fines and reputational damage. In order for organizations to demonstrate compliance with rules and regulations, they need to have effective security compliance monitoring and reporting. However, only a small percentage of respondents have formal metrics and reporting in place. Only 17 percent of E&R organizations consistently track and monitor the effectiveness of information security controls and have integrated reporting and measurement into their information security program. If an organization does not track the effectiveness of its compliance programs, it is difficult to be truly compliant. Managing risk in the new decade requires the ability to “demonstrate” being in control of risks, not just to “state” that it is so.

Outsourcing to third parties has outpaced security

The rise of outsourcing offers a number of important advantages, but it can also introduce significant risk; entrusting access to valuable assets to another organization. Yet, even though only 37 percent of respondents state that they are “very confident” in third party information security practices, only a small number (26 percent) perform regular third party testing. Moreover, only 11 percent have included this as top initiative in 2010. To manage this uncertainty, E&R organizations should consider regularly reviewing and testing vendor security capabilities, controls, and organizational dependencies. Third parties are an extension of the organization – and an organization is only as secure as its weakest link.

E&R organizations are late adopters of security technology and many critical technologies are under-deployed

E&R organizations are often not equipped with the latest security technology and thus their ability to mitigate risks may be limited. When asked which category best describes their organization’s adoption of security technology, the largest percentage of respondents (38 percent) state that they are “late majority”, meaning that they use technologies that are “proven”. But technology can only become proven over time; in the meantime, old hardware and out-of-date technology put data at risk.

Respondents’ answers reveal that several notable technologies may be under-deployed. For example, only 16 percent have “Data at rest security/encryption”; only 21 percent have “Email encryption”; only 24 percent have “Encrypted storage devices”; and only 41 percent have “Security log and event management systems”. Even though some of these technologies are being planned or even piloted, they are currently not in use, potentially placing data at risk.

The majority of E&R organizations do not have a business continuity management (BCM) strategy or plan

For E&R organizations, service continuity is critical. However, only 39 percent of organizations surveyed have a documented and approved business continuity strategy in place. This means that 61 percent of respondents either do not have a business continuity strategy, or do not know whether they have one. And it’s not enough to just have a plan on paper – to have value, it needs to be regularly tested and demonstrated. Yet 24 percent of respondents state that their business continuity plan has never been tested. In addition, in many of the entities responding to the survey, there is no clear leadership responsibility of the function: only 55 percent of respondents have at least one executive responsible for enterprise-wide business continuity management, which means that 45 percent are without one.

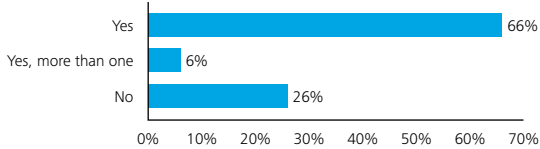
Detailed results

Governance

Existence of information security executive (CISO)

One of the key attributes of effective information security governance is the assigning of an executive responsible for information security; 72 percent of E&R organizations have such a person. Even though this is a slight increase from last year's survey, a quarter of all organizations in the E&R sector are still without such a role or its equivalent.

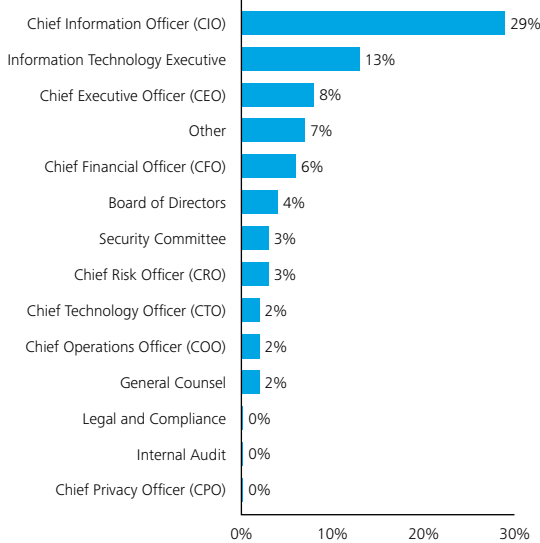
Figure 1 – Existence of a CISO



Reporting relationship of the CISO

Respondents indicate that the most common reporting relationship for the CISO is to the Chief Information Officer (CIO). While the majority of CISOs (54 percent) report directly to the Board of Directors or C-Suite, CISOs still report in aggregate (44 percent) to predominantly IT-related positions: CIO, CTO and IT executive. The reality remains that the CISO position is still considered by many to be an IT role.

Figure 2 – Reporting relationship of the CISO



Responsibilities of the CISO

The CISO's job is wide-ranging. Survey respondents indicate that the CISO's primary responsibilities are security governance, strategy and planning, and monitoring and compliance. Respondents indicate that CISOs are least responsible for conducting background checks, fraud management, physical security and business continuity planning.

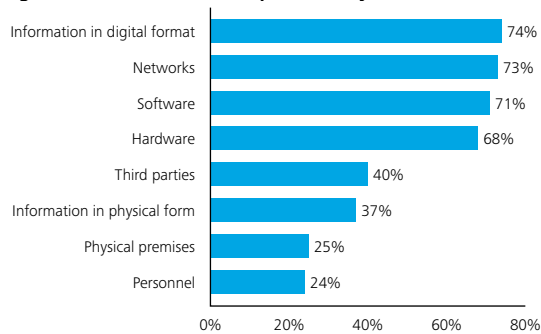
Figure 3 – Responsibilities of the CISO



Information assets protected by the CISO

Respondents indicate that the CISO's focus appears to be heavily weighted to digital assets, despite the evidence that loss of paper-based information (a prevalent form of information storage and most common in organizations that are considered late adopters of technology) and other information in non-digital format can have significant ramifications to the organization.

Figure 4 – Information assets protected by the CISO



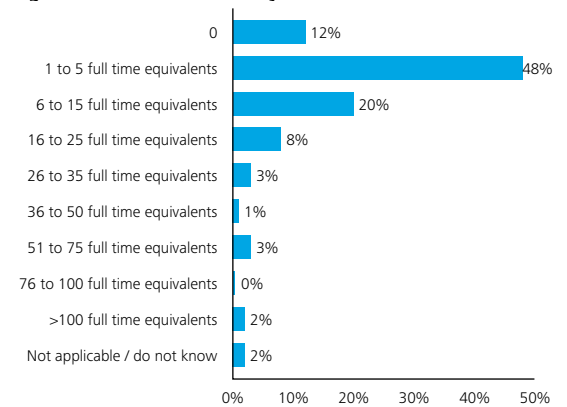
Information security competencies

The quest for qualified talent continues unabated. In this year's survey, 56 percent of respondents say their organization is missing skills and competencies to handle existing and foreseeable security requirements. To help address the problem, 52 percent of these organizations are supplementing their in-house capabilities with contractors and consultants to close the gap in competencies.

Information security function size

Information security functions continue to grow steadily. This year, 76 percent reported a headcount of up to 25 full-time security equivalents. However, 12 percent of the correspondents do not have any full-time security employees. This number is high when you take into account the scope and importance of initiatives that need to be undertaken to meet leading practices in information security.

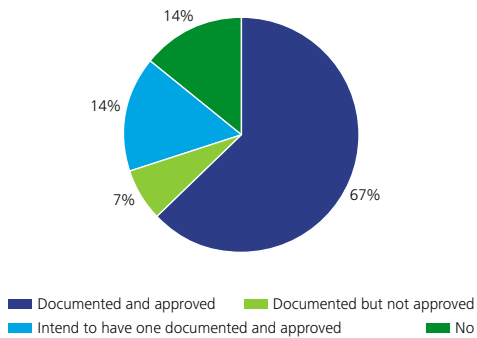
Figure 5 – Information security function size



Information security governance framework

A governance framework defines the roles and responsibilities, policies and procedures, guiding principles, and accountability requirements for managing information security. Most respondents (70 percent) already have such a framework, showing a small increase from last year's results. Another 16 percent of respondents intend to have one within the next 12 months.

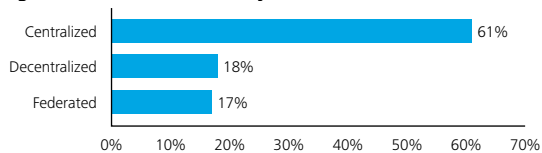
Figure 6 – Defined governance framework



Information security model structure

The majority (61 percent) of the information security functions use a centralized model, the traditional information security structure. The federated model (where a centralized group sets common standards and performs central functions while the business units maintain some control over "local" execution) accounts for 17 percent of respondents. In an age of increasing regulation and oversight as well as the impact of moving to more shared services centers, it is understandable that the decentralized model (18 percent) is low.

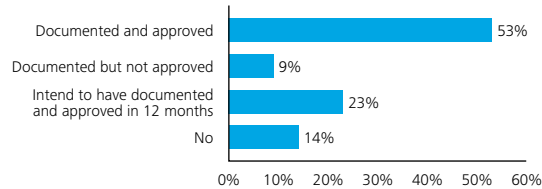
Figure 7 – Information security model structure



The information security strategy

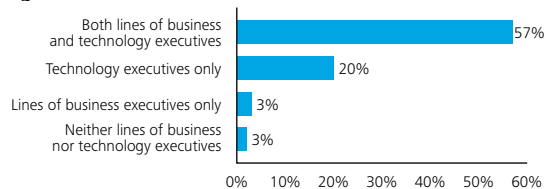
A prerequisite for effective information security is the implementation of an information security strategy that aligns the initiatives of the function with corporate initiatives. Such a strategy must be closely linked to the organization's overall business strategy, business requirements, and key business drivers. The survey reveals that 53 percent have a documented and approved information security strategy as opposed to 42 percent in 2008. This demonstrates that E&R organizations are heading in right direction. The remaining 47 percent either have a strategy documented but not approved, intend to have one documented and approved within the next 12 months or do not have one at all.

Figure 8 – The information security strategy



What is also important is not just that a strategy exists but also how it was created and how it is currently being implemented and followed. When asked whether the organization engages both lines of business and IT decision makers in identifying requirements for the organization's information security strategy, the majority of respondents (57 percent) engage both lines of business and IT decision makers. Almost one fifth (20 percent) of respondents engage IT decision makers only.

Figure 9 – Level of involvement of line of business



Top security initiatives for 2010

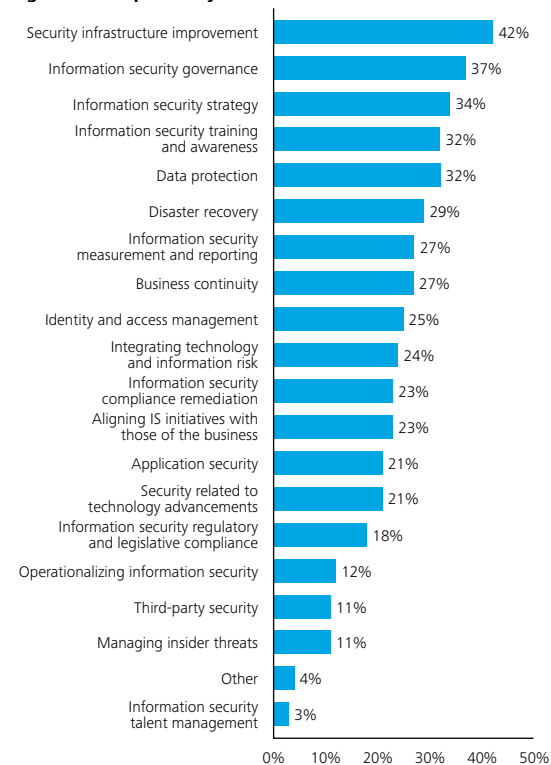
The most frequently mentioned security initiative (42 percent) in 2010 is security infrastructure improvement. This is not surprising since this was the top initiative in the previous year as well. However, while strengthening infrastructure is important, in many cases, the perpetrators of information systems compromise are already inside in the form of the organization's workforce. The good news is that this year, information security training and awareness has made it to the top five security initiatives, a factor that is expected to significantly help to institute an internal security mindset.

The second and third most frequently mentioned security initiatives are information security governance (37 percent) and information security strategy (34 percent) respectively. Organizations that are considering improving their existing governance and strategy are best to adopt industry approved information security and governance standards such as ISO 27001, COBIT and ITIL. These are proactive measures for data protection which show a growing maturity of the information security function. As evidence, data protection is a top five security initiative for the first time. The world has changed; information is now virtually every organization's lifeblood and data protection is where the focus must now lie. The increase in focus of this initiative can also be interpreted as a response to the events and security breaches that have attracted media attention over the last year. The spate of high-profile vulnerabilities highlighted by external storage media such as unprotected USB keys continues to make data protection more challenging. Devices such as these containing unencrypted data introduce opportunities to steal identities and gain access to confidential information.

Identity and access management fell from the second most frequently mentioned initiative to the ninth (25 percent) while business continuity fell from the third most frequently mentioned initiative to the eighth (27 percent). Additionally, information security regulatory and legislative compliance fell from fourth position to fifteenth (18 percent). Priorities have shifted dramatically this year and the focus is, at the same time, both reactive

and proactive: improving infrastructure (typically in reaction to an attempted or successful breach or a highlighted vulnerability) and creating a robust strategy that deals with setting the overall control framework and training employees (a proactive measure that sets policies and changes behavior).

Figure 10 – Top security initiatives for 2010



This year's results indicate that there is very little focus on third party security (11 percent). Given that E&R organizations heavily depend on outsourcing to third parties, this area represents a security gap, one that is rapidly being recognized and remedied by other industries. Third parties are extensions of the host organization; it is difficult for an organization to obtain confidence in its information security controls if it does not identify, monitor or test, those of its third parties.

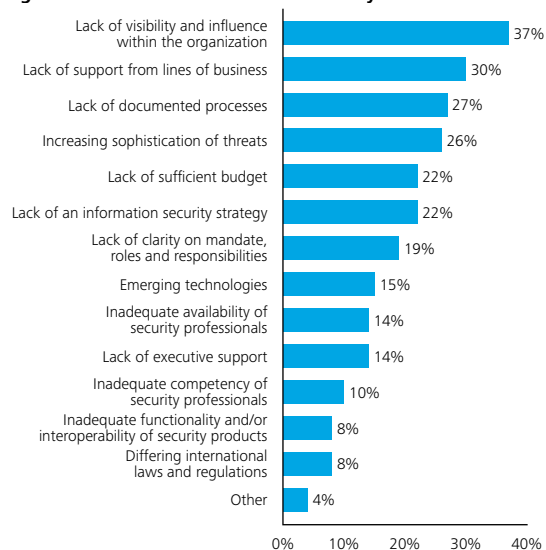
This year, a greater number of respondents to the survey have a documented and approved information security strategy than they did last year, confirming that Energy & Resources organizations are heading in right direction.

Major barriers to information security

The two most frequently mentioned barriers to ensuring information security are lack of visibility and influence within the organization and lack of support from lines of business of business.

Information security and the business must work closely together if there is to be continued progress in the information security domain. Awareness and training programs (one of the top security initiatives) will be expected to influence security attitudes and help to establish the reality that information security is an enterprise-wide issue and not just an IT issue. Involving the business in the IT security strategy and measuring and reporting on its effectiveness also helps to promote the visibility and influence of the function within the organization.

Figure 11 – Barriers to information security



Measuring the effectiveness of the information security program

In order to demonstrate effective information security governance, an organization must know and define its expected outcomes, performance targets, efficiency measures, and related reporting requirements. According to the survey, only 17 percent of EGR organizations consistently track and monitor the effectiveness of information security controls and have integrated reporting and measurement into their information security program.

One challenge with haphazard or no measuring is that it can be difficult to justify the information security program to the business. Hence, it is not surprising that respondents have rated “lack of visibility and influence within the organization” and “lack of support from lines of business” as two major barriers.

Reporting on the information security status of the organization

A purpose of reporting by the information security function should be primarily to capture the attention of the business. But this does not appear to be happening. When asked about the frequency of reporting on information security, a significant portion of respondents say that Senior and Executive management, the CEO, and the Board of Directors are provided with reports on information security on an ad hoc basis only. The problem with reporting when an incident occurs is that it is, in most cases, crisis-driven, meaning that the only time senior management hears about security is when it has ostensibly failed. Regular reporting, no matter how uneventful, is likely to give executives more peace of mind that security is under control.

Figure 12 – Measuring the effectiveness of the information security program

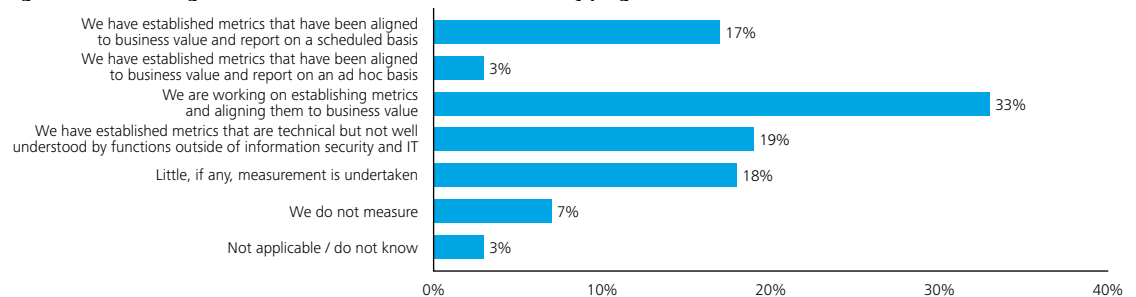


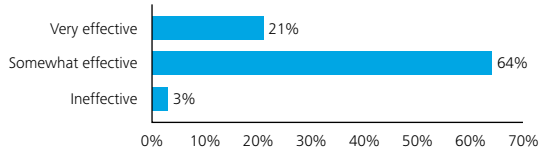
Figure 13 – Frequency of reporting on information security status to various parties

	Monthly	Quarterly	Semi-annually	Annually	Ad hoc	Never	Chose not to be informed
Board of Directors	7%	16%	5%	18%	32%	13%	0%
CEO	11%	18%	5%	9%	35%	8%	1%
Senior and Executive management	35%	19%	4%	5%	26%	5%	0%

Meeting the needs and expectations of the organization

If information security is not sufficiently valued within an organization, it is not likely to attract the resources that it needs. When asked how effective the information security function is at meeting the needs and expectations of the organization, 21 percent of respondents state that it is “very effective” while the majority (64 percent) state that it is only “somewhat effective”. This response could mean that most functions do not know what risks they face and may not know if the security policies and commensurate investment are truly meeting requirements.

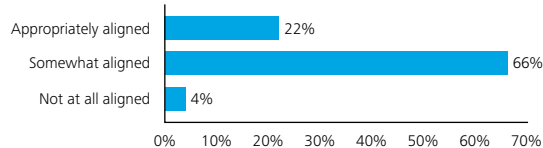
Figure 14 – Effectiveness of information security function in meeting the needs of the business



Alignment of information security and business initiatives

This is probably the finding that most reveals the maturity of any information security function – the extent to which its initiatives are aligned with those of the business. The largest percentage of respondents (66 percent) indicate that they are only “somewhat aligned” and only 22 percent state that they are “appropriately aligned”. With security governance a top five initiative, this is a significant improvement from last year’s results where 66 percent (compared to 88 percent this year) of respondents indicated that they are aligned or somewhat aligned.

Figure 15 – Alignment of information security and business initiatives



There is very little focus on third party security. Given that Energy & Resources organizations heavily depend on outsourcing to third parties, this lack of focus could represent a security gap, one that is rapidly being recognized and remedied by other industries.

Information security budget

IT budget dedicated to information security

Approximately 50 percent of respondents state that their information security budgets have increased; although the majority of increases are still in the lowest category (1 percent to 5 percent range). This trend is consistent with other industries that we have surveyed and may be the result of the anticipation of a recovering economy.

On the other hand, a considerable portion of respondents (26 percent) have had their budgets cut. This decline in security investment may not be enough to keep pace with the growing list of challenges, emerging technologies, and increasingly sophisticated attacks faced by companies.

Overall, year-over-year, lack of sufficient budget has become less of a barrier with only 22 percent of this year's respondents indicating that lack of sufficient budget is a major barrier compared to 35 percent last year.

Figure 16 – Information security budget trend

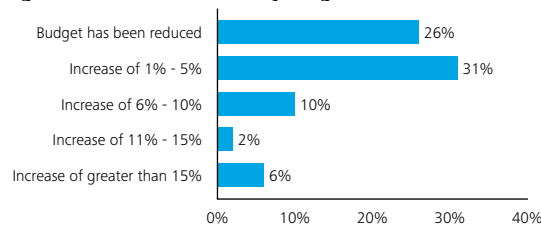
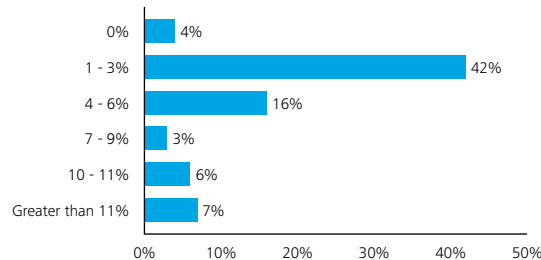


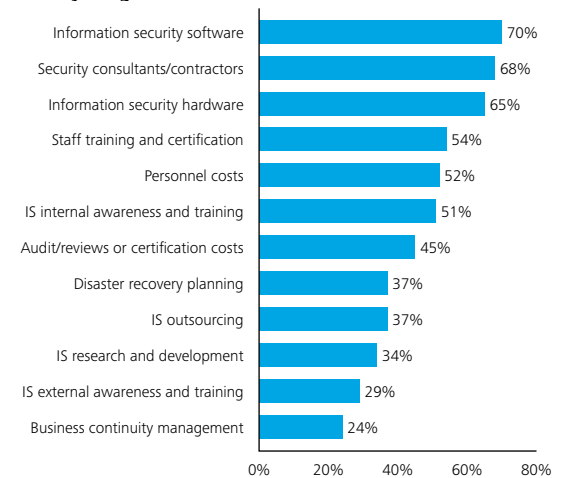
Figure 17 – Percentage of overall IT budget dedicated to information security



What is covered under the information security budget

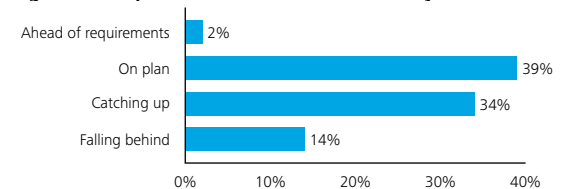
Not surprisingly, the vast majority of respondents indicate that software (70 percent) and hardware (65 percent) are covered under the information security budget with security consultants and contractors (68 percent) and training costs (54 percent) as the next greatest expenditures. These top areas are consistent with the top stated security initiatives.

Figure 18 – What is covered under the information security budget



The greatest majority of respondents (39 percent) characterize their expenditures on information security as "on plan". Very closely behind (at 34 percent) are those respondents who state that they are "catching up".

Figure 19 – Expenditures on information security



Threat landscape

Level of confidence in combating attacks

Like one's family, an organization's people are often the source of its greatest pride and its greatest worry. In general, external attacks are considered easier to deal with because they are performed by non trusted agents that do not have credentials or knowledge of the systems. On the other hand, internal attacks are far more challenging to deal with.

For external attacks, the majority of respondents (60 percent) indicate that they are either "extremely confident" or "very confident" in their ability to combat the threat; "somewhat confident" (38 percent) is the second most selected choice.

For internal attacks, it is a very different picture. Only 26 percent of respondents are either "extremely confident" or "very confident" and 49 percent of respondents are "somewhat confident".

Comparing the confidence levels of this year to the previous year's survey, we see that the confidence level for combating external attacks has slightly increased while the confidence level for combating internal attacks has decreased. The increase in confidence regarding external attacks may be attributable to the increase in technological investments; the decrease in confidence regarding internal attacks could be a dawning realization of the challenging nature of internal attacks and the fact that management now knows more about the wide and increasing range of risks presented by internal people on a daily basis. Hence, it seems logical that information security training and awareness has become one of the top five initiatives for this year.

Figure 20 – Confidence that your organization's information assets are protected from internal and external attacks

	Extremely confident	Very confident	Somewhat confident	Not very confident	Not confident at all
Attacks originating internally	2%	24%	49%	21%	3%
Attacks originating externally	6%	54%	38%	1%	1%

The survey reveals that the confidence level for combating external attacks has slightly increased while the confidence level for combating internal attacks has decreased.

Threat perception

Oil and gas industry breaches are usually focused on the crown jewels of the industry: valuable “bid data” detailing the quantity, value, and location of oil discoveries. We have also seen that attacks target all levels of an organization ranging from regular employees to C- suite executives. Therefore, when respondents were asked to rate the level of concern about malicious external threats on a scale of one to five, it was not surprising that “Increasing sophistication and proliferation of threats”, “Non-intentional loss of sensitive information” and “Employee errors and omissions” were ranked among the top threats.

One area of significant concern is threats that originate within the organization unintentionally which may, in most cases, affect the confidentiality, integrity or availability of information.

In order to counter emerging threats, organizations should try to minimize the probability of occurrence and limit the damage or impact caused by these threats. Looking back at the top security initiatives, the respondents surveyed in the E&R industry appear to have aligned their initiatives to counter these threats. “Security infrastructure improvement” is the top initiative, which will help counter Increasing sophistication and proliferation of threats. “Information security training and awareness”, the fourth top security initiative will help counter the second and third top threats.

Figure 21 – Threat rankings from highest to lowest threat

	Non-threat	Very low threat	A somewhat low threat	Average threat	Somewhat high threat	Very high threat
Increasing sophistication and proliferation of threats	1%	8%	14%	33%	29%	13%
Non-intentional loss of sensitive information	3%	11%	14%	27%	32%	9%
Employee errors and omissions	2%	4%	24%	42%	19%	5%
Phishing, pharming and other related variants	3%	16%	9%	38%	24%	7%
Employee abuse of IT systems and information	4%	8%	21%	31%	26%	5%
Attacks exploiting vulnerabilities of end point devices	5%	11%	20%	32%	27%	1%
Security breaches involving third party organizations	3%	15%	13%	31%	23%	7%
Social engineering	5%	14%	23%	30%	16%	8%
Exploits of vulnerabilities in emerging technologies	4%	16%	22%	30%	19%	5%
Zombie networks	3%	15%	32%	25%	16%	5%
Attacks exploiting vulnerabilities due to unsecured code	5%	14%	21%	31%	18%	5%
Differing cultural interpretations of security positive behavior	7%	13%	18%	38%	16%	3%
External financial fraud involving information systems	8%	31%	18%	19%	18%	4%
State or industrial espionage	10%	31%	16%	18%	20%	3%
Insider and rogue trading	8%	24%	19%	34%	9%	1%

Occurrence of breach incidents

Almost half of respondents (49 percent) in the E&R industry indicate that they have experienced at least one external breach in the last 12 months; 40 percent have not. Occurrences of internal breaches were almost equally frequent as external attacks. Just about half of respondents (48 percent) indicate that they have experienced at least one internal breach in the last 12 months; 41 percent have not.

Figure 22 – Occurrence of an external breach incident in the last 12 months

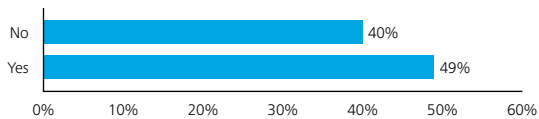
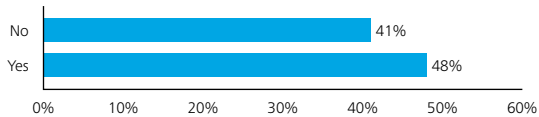


Figure 23 – Occurrence of an internal breach incident in the last 12 months



One interesting fact is that the respondents indicated that the repeated occurrence of “Breach of information originating from inside the organization conducted by an employee” (9 percent) is significantly higher than the repeated occurrence of “Breach of information originating from outside the organization” (0 percent). This shows that once external breaches had been detected, preventive action was taken to prevent further breaches. Moreover, the top five initiatives for this year may better equip E&R organizations to address the threats generated internally since the top initiatives address both technology and people.

By far, the greatest number of respondents (29 percent) identified “malicious software originating outside the organization” as the most common repeated external breach type. Internally, the greatest number of respondents (23 percent) identified “Accidental breach of information originating from inside the organization” as the most common repeated internal breach type. Accidental breaches may be caused by an error on the job because of a lack of documented procedures which cause the information to be compromised.



Figure 24 – Nature and frequency of external breaches

	Repeated occurrences	One occurrence
Theft of information resulting from state or industrial espionage	1%	7%
External financial fraud involving information systems	2%	2%
Breach of information originating from outside organization	0%	5%
Loss of information originating from a physical attack outside the organization	21%	3%
Breach of information originating from a third party vendor	4%	4%
Mobile network breach originating from outside the organization	1%	3%
Malicious software originating from outside the organization	29%	11%
Website defacement	2%	7%
Other form of external breach	1%	8%

Figure 25 – Nature and frequency of internal breaches

	Repeated occurrences	One occurrence
Internal financial fraud involving information systems	5%	3%
Insider and rogue trading	1%	2%
Breach of information originating from inside the organization conducted by an employee	9%	11%
Breach of information originating from inside the organization conducted by a non-employee	1%	5%
Accidental breach of information originating from inside the organization	23%	5%
Breach of information originating from a third party vendor	4%	8%
Mobile network breach originating from inside the organization	2%	7%
Malicious software originating from inside the organization	14%	10%
Other form of internal breach	2%	0%

The occurrence of breaches of information originating from inside the organization (9 percent) is significantly higher than those originating from outside (0 percent).

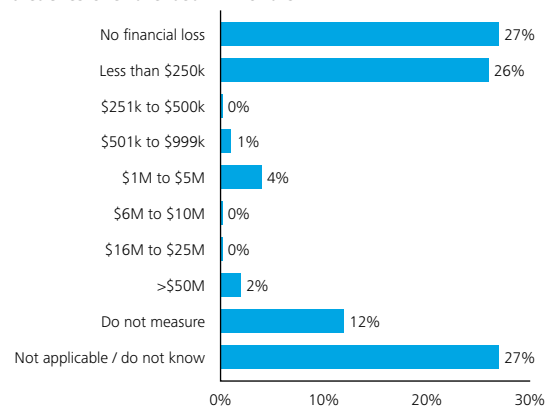
More than half of respondents (60 percent) conduct vulnerability scanning either quarterly, semi-annually or annually.

Monetary damage resulting from breaches

The costs (direct and indirect) of damage sustained as a result of these breaches have not been significant over the past 12 months. For most organizations (26 percent) that measure, the figure was less than \$250,000. However, a substantial number of organizations (27 percent) said that they did not know the full cost and 12 percent said that they did not measure it systematically. A small minority of respondents (5 percent) said that they have experienced significant losses from breaches in the range of \$501k to \$5M.

The main factors included within the calculation to determine the monetary damages include “Lost employee productivity costs”, “Internal investigation and forensic costs” and “Remediation costs (including consultants)”.

Figure 26 – Estimated total monetary damages resulting from breaches over the last 12 months



Types and frequency of security testing

More than half of respondents (60 percent) conduct vulnerability scanning either quarterly, semi-annually or annually while almost one quarter of respondents do so only on an ad hoc basis (26 percent). Nine percent (compared to 5 percent in 2008) indicate that they never perform vulnerability scanning.

Penetration testing and application code reviews are conducted less frequently than vulnerability scanning – 30 percent to 40 percent of organizations do so only on an ad hoc basis and 31 percent never test applications. This weakness, where organizations pay no attention to application security, is also present in other industries such as the financial and technology industries.

Figure 27 – Types and frequency of security testing

	Quarterly	Semi-annually	Annually	Adhoc	Never
Vulnerability scanning	32%	10%	18%	26%	9%
Internal penetration testing	15%	12%	18%	33%	16%
External penetration testing	11%	13%	22%	36%	11%
Penetration testing conducted by third party	9%	13%	26%	30%	13%
Application security code review	5%	5%	2%	40%	31%

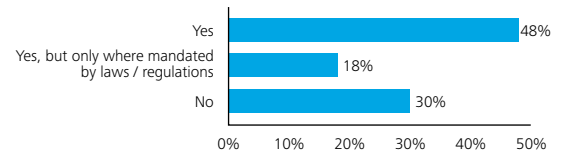


Most employees of Energy & Resources organizations (66 percent) have received at least one training program on identifying and reporting suspicious activities.

Training

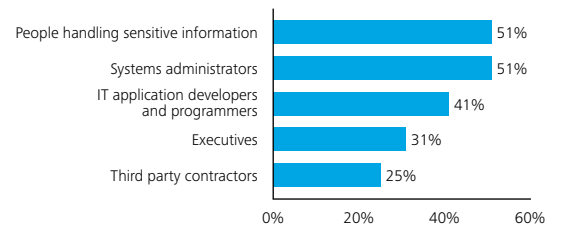
Most employees of E&R organizations (66 percent) have received at least one training program on identifying and reporting suspicious activities. These training sessions are mostly aimed at internal employees who are dealing with sensitive information (system administrators: 51 percent, people handling sensitive information: 51 percent, IT application developers and programmers: 41 percent) compared to other groups (executives: 31 percent and third parties: 25 percent).

Figure 28 – Train employees on identifying and reporting suspicious activities



Information security training and awareness is one of the top five security initiatives which bodes well for a significant improvement in this area.

Figure 29 – Percentage of employees trained by job role and function



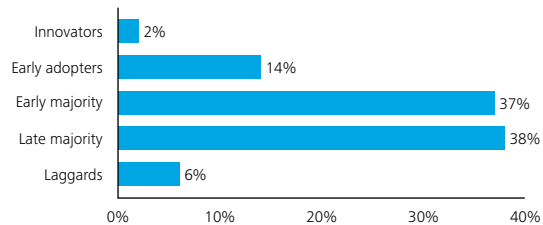
Use of security technologies

Rate of adoption

Although there are advantages to being on the forefront of technology, new technology developments do not always deliver what they promise. On the other hand, proven technology may be perceived as a 'safe bet,' yet may be only months away from obsolescence given the startling pace of technology development.

In terms of adopting new technologies, 14 percent of respondents are "early adopters"; 37 percent are "early majority" (e.g., may experiment on ad hoc basis); 38 percent are "late majority" (e.g., users of proven and effective technologies); and 6 percent are "laggards". The results are very similar to last survey's result and this shows that a substantial number of organizations prefer to work with proven technologies. To stay ahead of the threats and as appropriate for the company's purposes, EGR organizations should continue to adopt new security technologies.

Figure 30 – How organizations characterize their adoption of security technologies



Types of security technologies

Predictably, an overwhelming majority of respondents indicate that their organizations employ firewalls (98 percent), antivirus (97 percent), spam filtering solutions (90 percent) and anti spyware software (82 percent).

However, several notable technologies may be under deployed. For example, only 16 percent have "Data at rest security/encryption"; only 18 percent have "Federated identity management "; only 19 percent have "Data loss prevention technology "; only 21 percent have "Email encryption"; only 24 percent have "Encrypted storage devices "; and only 41 percent have "Security log and event management systems".

The top technologies being piloted are:

- Security log and event management systems (23 percent)
- Email encryption (21 percent)
- Data loss prevention technology (21 percent)

The top technologies that organizations are planning to pilot or have fully deployed within the next 12 months are:

- Encrypted storage devices (26 percent)
- Biometric technologies for user authentication (25 percent)
- Data loss prevention technology (25 percent)
- File encryption for mobile devices (25 percent)
- Enterprise Single Sign on (25 percent)
- Security compliance tools (25 percent)

The top technologies being piloted are security log and event management systems (23 percent), email encryption (21 percent) and data loss prevention technology (21 percent).

Figure 31 – Security technologies deployed, piloted and planned

	Fully deployed	Currently piloting	Plan to fully deploy or pilot within 12 months
Firewalls	98%	0%	1%
Antivirus	97%	0%	2%
Spam filtering solutions	90%	3%	2%
Anti spyware software	82%	5%	7%
Content filtering/monitoring	75%	9%	7%
IDS/IPS	60%	14%	12%
Anti phishing solutions	51%	10%	15%
Vulnerability management	49%	14%	16%
Wireless security solutions	48%	8%	16%
Network access control	44%	5%	19%
Web access management systems	42%	9%	14%
Security log and event management systems	41%	23%	19%
Network behavior analysis	35%	10%	19%
Email authentication	33%	15%	16%
Incident management workflow tools	32%	5%	21%
Email encryption	27%	21%	22%
File encryption for mobile devices	27%	13%	25%
Web services security	26%	10%	16%
Encrypted storage devices	24%	16%	26%
Enterprise Single Sign On	23%	14%	25%
Security compliance tools	21%	8%	25%
Data loss prevention technology	19%	21%	25%
Federated identity management	18%	9%	22%
Data at rest security/encryption	16%	13%	22%
Biometric technologies for user authentication	5%	9%	25%

Business Continuity Management (BCM)

Business continuity strategy

For E&R organizations, service continuity is critical to success. However only 39 percent of surveyed E&R organizations state that they have a documented and approved business continuity strategy in place. That means 61 percent of respondents either do not have a BCP, or do not know about it.

To understand why a significant portion of E&R organizations have not established something as critical as a business continuity program, we must look at the major of barriers cited by the respondents:

- Lack of support from lines of business (21 percent)
- Lack of visibility and influence within the organization (20 percent)

It seems as though E&R organizations are lacking a unified vision with the different lines of business. Moreover, 51 percent of organizations indicate that there is limited integration of business and technology plans. One recommendation that could help overcome this barrier would be for organizations to establish a BCM steering committee with executive management support. Survey results show that only 23 percent of respondents have such a committee.

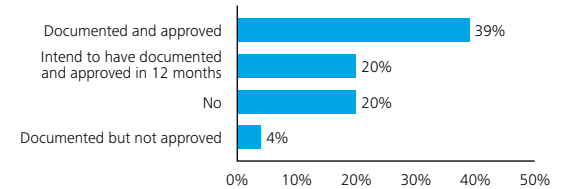
Respondents indicate that the three major drivers for business continuity planning are:

- Ensuring operational resiliency and availability (60 percent)
- Regulatory compliance (25 percent)
- Protecting public image or reputation (21 percent).

Respondents state that 55 percent of their E&R organizations have at least one executive responsible for enterprise-wide BCM. However, one third of respondents admit that their staff is missing competencies (e.g., knowledge, certifications, skills and behaviors) to handle business continuity responsibilities and better ensure compliance with applicable requirements.

Organizations that have developed BCM have also established BCM related teams/roles including emergency response team (53 percent), crisis management (51 percent), business continuity recovery teams (44 percent), disaster recovery teams (58 percent) and pandemic readiness teams (33 percent).

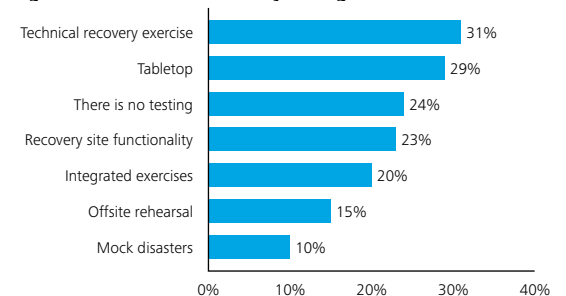
Figure 32 – State of Business Continuity Strategy



Testing of business continuity

A business continuity plan may satisfy a need on paper, but to really have value, it needs to be tested and demonstrated. Yet 24 percent of respondents say their business continuity plan has never been tested. For some respondents, regular testing is performed but mostly (20 percent) on the disaster recovery components and not all the components of the business continuity plan. Also, 47 percent of organizations do not employ metrics to measure the effectiveness of their BCM initiatives.

Figure 33 – Business Continuity testing



Outsourcing and third party security management

Today, nearly all organizations have outsourced some of their business processes. Only 12 percent of respondents (compared to 33 percent last year) indicate that they do not outsource any type of security activities. This shows that the majority of E&R organizations are relying more and more on outsourcing security functions.

Significant functions that organizations outsource include: Security technology services, Vulnerability management and application management services. Cyber threat intelligence vendors are pushing their managed security services aggressively especially with the oil and gas organizations, therefore it is not surprising that “Threat management and Monitoring services” and “Threat risk assessments” are part of the top outsourced activities.

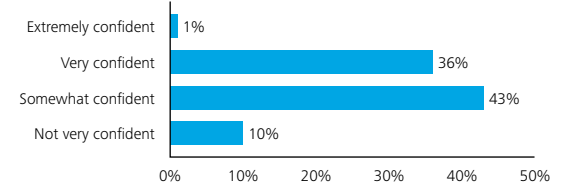
Figure 34 – Functions that your organization outsources



Confidence in third party information security practices

Only 36 percent of respondents are “very confident” in their third parties’ information security practices, while 53 percent of respondents indicate “not very confident” or “somewhat confident”. Obviously, vendors have a strong vested interest in making sure that their relationship with the host organization is beyond reproach from a security standpoint. However, since the majority of internal breaches are a result of inadvertent and careless behavior rather than malicious intent, third parties face many of the same issues relating to their personnel as the organizations they contract with.

Figure 35 – Confidence in third party information security practices



Today, nearly all organizations have outsourced some of their business processes. Only 12 percent of respondents (compared to 33 percent last year) indicate that they do not outsource any type of security activities.

Knowledge of third-party security capabilities, controls and organizational dependencies

When an E&R organization relies on third parties to handle parts of its information security, how can it assess whether the third parties' information security practices are reliable? Ideally, third party relations and capabilities should be periodically reviewed and tested to assess whether these extended business relationships are delivering as promised. Yet according to the survey results, only 26 percent of respondents do such reviews and testing on a regular basis.

Ensuring third-party security practices

By far, the most common way (66 percent) respondents use to ensure third party security practices is by having the third party sign a confidentiality or non-disclosure agreement. The next most common way (52 percent) is to control what access third parties have to systems and data. Again, there may be a false sense of security about third parties because some rely on the third-party's best intentions or its limited use of, or access to, information. However, as has been discussed, human nature can foil even the best of intentions and accidents can happen. Insistence on robust monitoring should be considered as another option by organizations.

Figure 36 – Knowledge of third-party security capabilities, controls and organizational dependencies

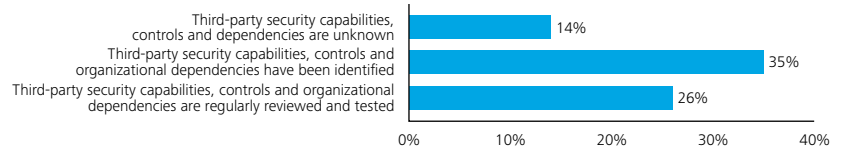
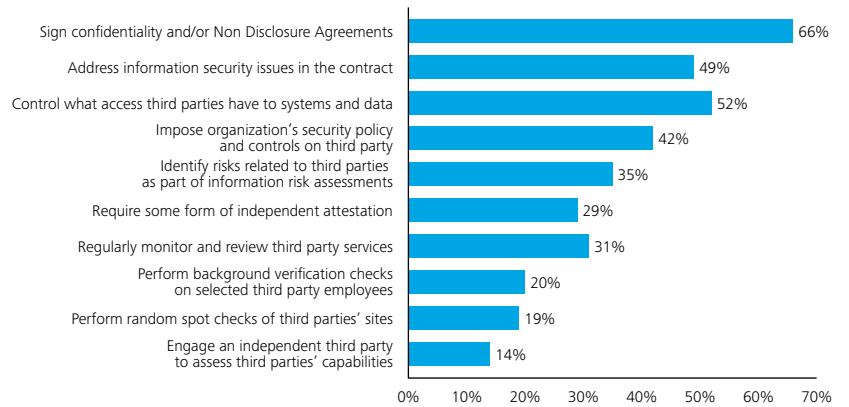


Figure 37 – Ensuring third-party security practices



Privacy

Existence of Chief Privacy Officer

The largest percentage of respondents state that they do not have a Chief Privacy Officer (47 percent). However, as privacy and data protection legislation for the industry increases, it is likely that this position will become more common.

The reporting structure for the privacy executive is mainly to the CEO (8 percent), CIO (7 percent), general counsel (7 percent), legal and compliance (6 percent), and board of directors (5 percent). This demonstrates the increasing importance of this role and its visibility at the top of organizations.

Maturity of privacy program

Coincident with the low number of respondents who indicate that they do have a Chief Privacy Officer, the highest numbers of respondents (36 percent) indicate that their privacy program is immature – they actually do not have a defined full-fledged privacy program in place. The maturity of the privacy function is likely to be driven by regulation.

Managing privacy

The greatest percentage of respondents (40 percent) do not have a program for managing privacy compliance. This may become a big concern going forward – in an era of stiff competition, organizations collect, store, and process data over a period of many years. If there is no operational privacy program in place, personally identifiable information (PII) may be at risk. Although most respondents do not have a developed privacy function or a Chief Privacy Officer position, the greatest number of respondents (55 percent) indicate that they have a written privacy, fair information practices or data collection policy in place. Again, despite the lack of a developed privacy function or a Chief Privacy Officer, the greatest number of respondents (43 percent) indicate that they have formal directives with respect to the destruction of personal information.

In an era of stiff competition, organizations collect, store, and process data over a period of many years. If there is no operational privacy program in place, personally identifiable information (PII) may be at risk.

A large number of respondents (31 percent) indicate that they do not have a formal process to deal with complaints about personal information management practices. The problem with this lack of a process is that there may be no way of using feedback to improve practices or respond to complaints.

Figure 38 – Maturity of privacy program

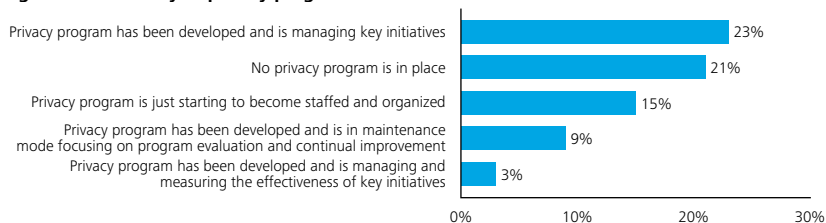


Figure 39 – Managing privacy

	Yes	No	N/A, do not know
A program for managing privacy compliance	36%	40%	20%
A written privacy, fair information practices or data collection policy in place	55%	27%	12%
Formal directives in place with respect to the destruction of personal information	43%	30%	24%
A formal process in place to deal with complaints about personal information management practices	42%	31%	24%

Compliance

Internal/external audit findings

The top internal/external audit findings indicated by the respondents over the prior 12 month period were

- Excessive access rights (40 percent)
- Lack of sufficient segregation of duties (35 percent)
- Ineffective password management (30 percent)
- Business continuity and disaster recovery (27 percent)
- Audit trails/logging issues (25 percent)

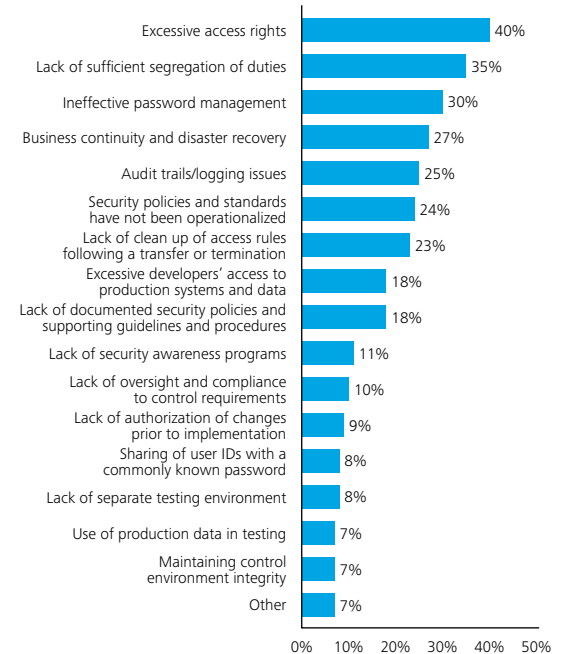
“Excessive access rights” is the top audit finding this year compared to “Lack of documentation of controls”, the top finding of last year. This likely means that the vast majority of E&R organizations may have put a significant amount of effort into defining and establishing documentation, such as security policies, supporting guidelines and procedures.

“Excessive access rights” is probably going to remain an important topic for some time. Auditors and regulators expect that individuals will have access only to the information that is needed to perform their jobs. As simple as this sounds, in theory, it is not. Given changing job responsibilities, a more mobile workforce, employee turnover and corporate reorganizations, this may be a tall order.

“Segregation of duties” is an important information security control. There is a lack of segregation of duties when one individual has access to responsibilities that are inherently in conflict with one another. For example, the same person should not accept cash, record deposits, make deposits, and reconcile the bank account. It is a lack of segregation of duties that may allow some individuals to undertake embezzling schemes that go unnoticed for years.

The top two audit findings may signify weaknesses in user access management; however, “identity and access management” was not one of the top initiatives for this year.

Figure 40 – Internal/External audit findings



Respondents indicate that password management has been identified as a weakness in their organizations. Single Sign On and Biometric technology for user authentication are some of the technologies that a large portion of respondents plan to pilot or have fully deployed within the next 12 months. If deployed properly, these technologies can significantly alter the way passwords are managed and increase security substantially.

Executive support for projects

With regard to senior executive support of security projects to address regulatory and legal requirements, roughly 51 percent of the organizations say that they are receiving adequate funding and support for projects. However, 28 percent indicate that they receive support but no funding while 1 percent say there is neither commitment nor funding.

Energy and resources specific questions

Industrial control IT infrastructure

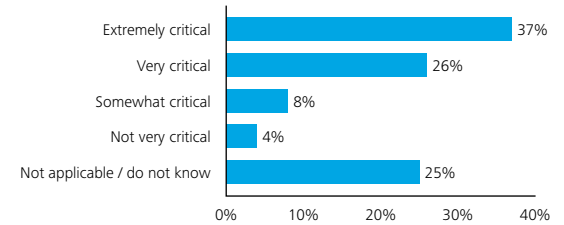
Respondents were asked a series of questions specific to the E&R industry. One way in which the sector is differentiated from others is by its dependence on industrial control IT systems such as Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS) and Process Control Network (PCN) – systems that are typically used to monitor or control manufacturing and transport processes.

As industrial control IT systems are becoming more 'connected', so are the cyber-attacks by means of network intrusions, malicious codes and unauthorized access. The subsequent consequences are profound for the security of the industrial systems in place such as the electrical grid. Regulatory bodies and governments have started to focus on this risk area. In a recent collaboration between North American Electric Reliability Corporation (NERC) and US Department of Energy (DOE)², a Coordinated Action Plan was drafted to address coordinated cyber-attacks that disrupt or impair the integrity of multiple industrial control systems.

There is little doubt that organizations in the sector see their industrial control IT infrastructure as being critical to their business: 37 percent of respondents describe it as "extremely critical", 26 percent as "very critical" and 8 percent as "somewhat critical". We note this is a drop from a previous survey where 45 percent of the respondents noted this as "extremely critical". This decrease may be attributed to two factors:

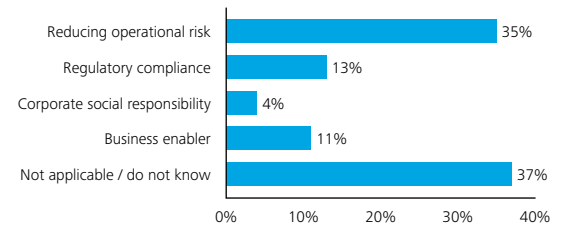
- Processes supported by SCADA are evolving and are using technologies that are IP based.
- In the past few years, increasing attention has been given to processes supported by SCADA systems. This has helped add several security layers and manual processes that are built to address disruptions to the processes.

Figure 41 – Criticality of the security of industrial control IT infrastructure



The largest percentage of respondents (35 percent) say that the top business driver for industrial control IT infrastructure risk management is to reduce operational risk.

Figure 42 – Influential drivers with respect to security



While the largest percentage of respondents indicate that they are confident in the security of their industrial control IT infrastructure, a considerable percentage (29 percent) state that they are merely "somewhat confident", while 9 percent confess that they are not confident at all. This represents a 6 percent decrease in the confidence level from a previous survey which may show that a suitable risk management program is required to help assess the security of their industrial control IT environments.

² <http://www.nerc.com/files/HILF.pdf>

Almost half of organizations (44 percent) say they conduct vulnerability assessments on their industrial control IT environment, that is, they check for weak configurations, unapplied patches, or design weaknesses.

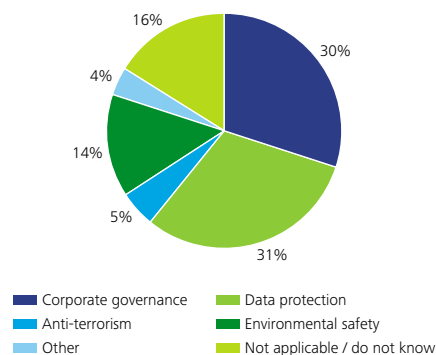
Almost half (47 percent) of organizations participating in the survey have an information risk management process for industrial control IT environments. However, only 27 percent indicate that they are “very aligned” or “completely aligned” with the enterprise-wide information security governance program. This substantiates our theory that a more robust and transparent information risk management process for industrial control IT environments may be required.

Almost half of organizations (44 percent) say they conduct vulnerability assessments on their industrial control IT environment, that is, they check for weak configurations, unapplied patches, or design weaknesses.

When asked to rate the most significant information security incident involving industrial control IT infrastructure over the prior 12 months, the most frequent response (32 percent) was that organizations have not experienced such incidents. However, 8 percent have experienced a serious incident.

Also, half of organizations feel that the security needs of their industrial control IT infrastructure are adequately considered by current suppliers of industrial control solutions. By far, the most significant influential drivers with respect to security are data protection (31 percent) and corporate governance (30 percent). These two drivers are consistent with the top E&R security initiatives of this year.

Figure 43 – Top business driver for industrial control IT infrastructure



The top two audit findings signify weaknesses in user access management.

How the survey was designed, implemented and evaluated

Drafting of the questionnaire

The questionnaire was comprised of questions composed by a global survey team made up of senior Deloitte member firm Information & Technology Risk Services professionals. Questions were selected based on their potential to reflect the state of information security and privacy in the E&R industry. The questions were chosen for global suitability, timeliness and value.

The collection process

Once the questionnaire was finalized and agreed upon by the survey team, questionnaires were distributed to the participating regions electronically. Data collection involved gathering both quantitative and qualitative data from respondents related to the identified areas. Member firms in each participating region assigned responsibility to senior members of their Information & Technology Risk Services practices and those people were charged in obtaining answers from the E&R organizations. Most of the data collection process took place through face-to-face interviews with the Chief Information Security Officer/ Chief Security Officer (CISO/CSO) or designate and in some instances with the security management team. Deloitte member firms also offered pre-selected E&R organizations the ability to submit answers online using a questionnaire managed by DeloitteDEX Advisory Services.

Results analysis and reporting

This report has been developed based on the participants' responses to the study questionnaire. Deloitte has elected to include data that we believe will be most meaningful and relevant to the reader; therefore, this report does not include all the questions and responses from the study questionnaire.

Specific responses were eliminated from the data included in the charts. "Do not know" responses were not included in the data and, in certain cases, where respondents were asked to indicate actions they were taking or areas they were concerned about or focused on, only the top responses were included.

Additional insights

As the amount of data collected during 2010 E&R Global Security Study far exceeds the boundaries of this publication, it reports only on the most important data points at an aggregate level. The study team encourages you to contact your local Deloitte member firm Information & Technology Risk practitioners for further insights on security practices within your industry, sub-sector, region, country, or a peer group of organizations.

Acknowledgements

The Energy & Resources practices of Deloitte member firms wish to thank all of the professionals of the Energy & Resources institutions who responded to this year's survey and who allowed us to further correspond with them over the course of this project. Without such participation and commitment, these practices would not be able to produce surveys, such as this. The Energy & Resources practice extends its heartfelt thanks for the time and effort that respondents devoted to this project.

Survey development team

Content

Tariq Ajmal

Deloitte Middle East
+971 2 676 0025
tajmal@deloitte.com

Fadi Mutlak

Deloitte Middle East
+971 4 369 8999
fmutlak@deloitte.com

Georges Ghanem

Deloitte Middle East
+971 4 369 8999
geghanem@deloitte.com

Data collection

DeloitteDEX

Olivier Curet

Deloitte United States
(Deloitte & Touche LLP)
+1 216 589 5448
ocuret@deloitte.com

Sheila Celata

Deloitte United States
(Deloitte & Touche LLP)
+1 617 437 2128
scelata@deloitte.com

Marketing support

Jonquil Peel

Deloitte Canada
+1 416 601 4831
jpeel@deloitte.ca

Mark L Robinson

Deloitte Touche
Tohmatsu Limited
+1 703 251 4057
mlrobinson@deloitte.com

Contributors

Adel Melek

Deloitte Canada
+1 416 601 6524
amelek@deloitte.ca

Simon X Owen

Deloitte United Kingdom
+44 20 7303 7219
sxowen@deloitte.co.uk

Adnan Amjad

Deloitte United States
(Deloitte & Touche LLP)
+1 713 982 4825
aamjad@deloitte.com

Walter Carlton

Deloitte United Kingdom
+44 131 535 7244
wcarlton@deloitte.co.uk

Andrei Kananovich

Deloitte Canada
+1 416 874 4125
akananovich@deloitte.ca

Contacts

Global leaders

Peter Bommel

Global Industry Leader
Energy & Resources
Deloitte Touche Tohmatsu Limited
+31 882 880 935
pbommel@deloitte.nl

Mark Layton

Global Managing Director
Enterprise Risk Services
Deloitte Touche Tohmatsu Limited
+1 214 840 7979
mlayton@deloitte.com

Adel Melek

Global Managing Director
Information & Technology Risk
Deloitte Touche Tohmatsu Limited
+1 416 601 6524
amelek@deloitte.ca

George Cambanis

Global Shipping Leader
Deloitte Touche Tohmatsu Limited
+30 201 678 1226
gcambanis@deloitte.gr

Pat Concessi

Global Climate Change & Carbon Markets
Deloitte Touche Tohmatsu Limited
+1 416 601 6251
pconcessi@deloitte.ca

Dick Cooper

Global Leader
Energy & Resources Consulting
Deloitte Touche Tohmatsu Limited
+1 403 261 8115
dcooper@deloitte.ca

John England

Global Leader E&R Industry
Enterprise Risk Services
Deloitte Touche Tohmatsu Limited
+1 713 982 2556
jengland@deloitte.com

Phil Hopwood

Deloitte Touche Tohmatsu Limited
Global Mining Leader
+61 3 9671 6461
phopwood@deloitte.com.au

Adi Karev

Deloitte Touche Tohmatsu Limited
Global/China Leader Oil & Gas
+852 2852 6442
adikarev@deloitte.com.hk

Security, Privacy, & Resiliency

regional leaders

Americas

Nick Galletto

Deloitte Canada
+1 416 601 6734
ngalletto@deloitte.ca

Rhoda Woo

Deloitte United States
(Deloitte & Touche LLP)
+1 212 436 3388
rwoo@deloitte.com

Martin Carmuega

Deloitte Argentina
+54 11 43204003
mcarduega@deloitte.com

Asia Pacific

Uantchern Loh

Deloitte Singapore
+65 6216 3282
uloh@deloitte.com

Europe, Middle East & Africa

Simon X Owen

Deloitte United Kingdom
+44 20 7303 7219
sxowen@deloitte.co.uk

Regional contacts

Americas

Nick Galletto

Deloitte Canada
+1 416 601 6734
ngalletto@deloitte.ca

Paul Zonneveld

Deloitte Canada
+1 403 503 1356
pzonneveld@deloitte.ca

Adnan Amjad

Deloitte United States
(Deloitte & Touche LLP)
+713 982 4825
aamjad@deloitte.com

Steve Livingston

Deloitte United States
(Deloitte & Touche LLP)
+206 716 7539
slivingston@deloitte.com

Andre Gargaro

Deloitte Brazil
+55 11 5186 1268
agargaro@deloitte.com

Mauricio Torres Romero

Deloitte Mexico
+52 55 50806943
mtorresromero@deloittemx.com

Asia Pacific

Joshua Chua

Deloitte Singapore
+65 6216 3188
joshuachua@deloitte.com

Vishal Chawla

Deloitte India
+1 703 251 1793
vchawla@deloitte.com

Danny Lau

Deloitte Hong Kong
+852 2852 1015
danlau@deloitte.com.hk

Tommy Viljoen

Deloitte Australia
+61 02 9322 7713
tfviljoen@deloitte.com.au

Europe, Middle East & Africa

Kris Budnik

Deloitte South Africa
+27 0 11 806 5224
kbudnick@deloitte.co.za

Mike Maddison

Deloitte United Kingdom
+44 20 7303 0017
mmaddison@deloitte.co.uk

Colm McDonnell

Deloitte Ireland
+353 1 417 2348
cmcdonnell@deloitte.ie

Alfonso Mur

Deloitte Spain
+34 915145000 x2103
amur@deloitte.es

Chris Norman

Deloitte France
+33 1 51 61 47 72
cnorman@deloitte.fr

Sven Probst

Deloitte Switzerland
+41 44 421 6401
sprobst@deloitte.ch

Carsten Schinschel

Deloitte Germany
+49 211 8772 3163
cschinschel@deloitte.de

Hans Bootsma

Deloitte Netherlands
+31 88 288 1546
hbootsma@deloitte.nl

Chris Verdonk

Deloitte Belgium
+32 2 800 24 20
cverdonk@deloitte.com

Tariq M. Ajmal

Deloitte Middle East
+971 2 676 0025
tajmal@deloitte.com

Paul O'Brien

Deloitte Russia
+7 495 787 0600
paulobrien@deloitte.ru

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 170,000 professionals are committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

© 2011 Deloitte Global Services Limited

Designed and produced by The Creative Studio at Deloitte, Canada. 11-817G