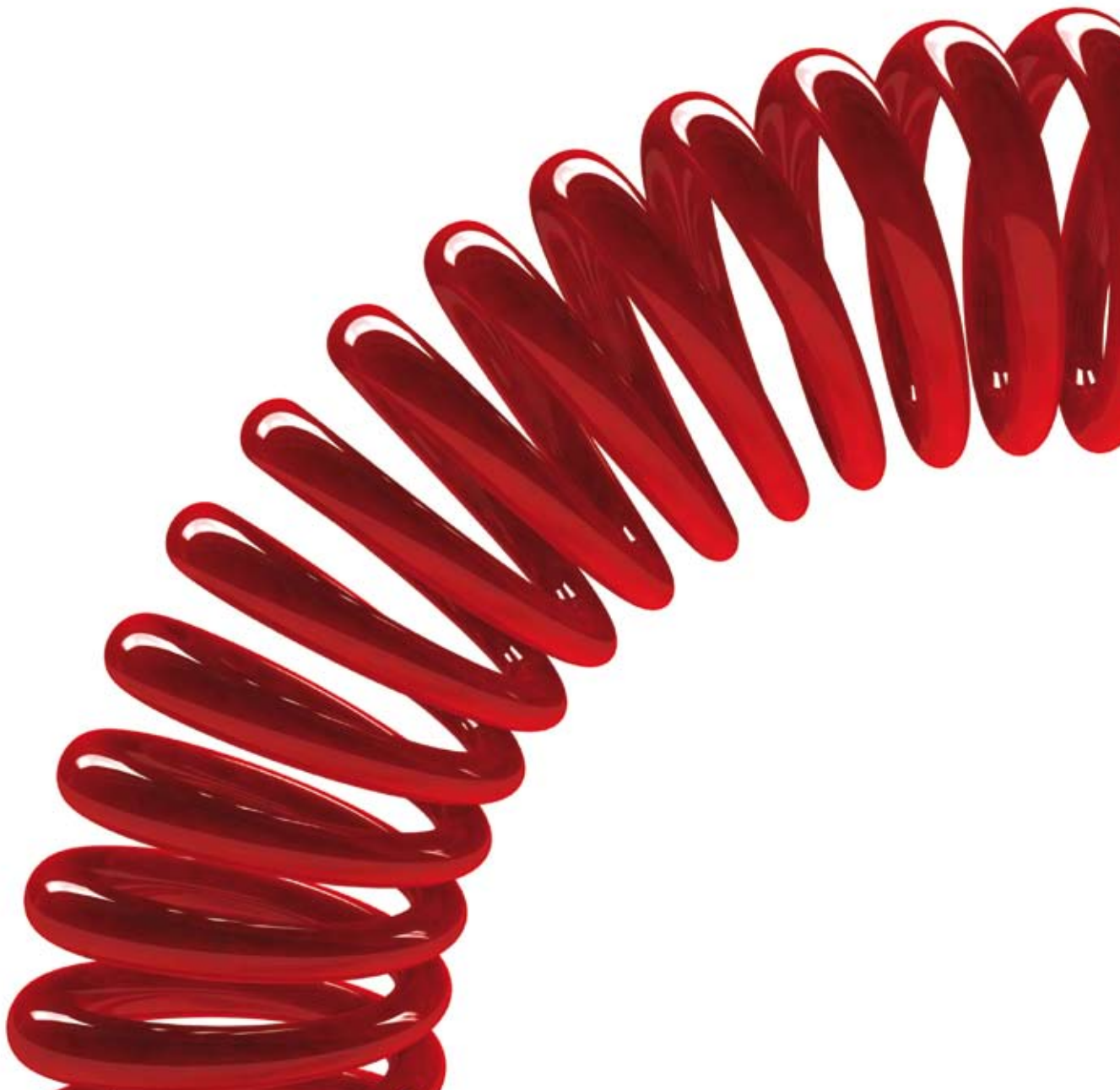




2010 TMT Global  
Security Study - Key findings  
Bounce Back







# Foreword and Summary

Welcome to the fourth edition of the Global Security Study for the Technology, Media & Telecommunications (TMT) industry. The study is based on in-depth research and detailed interviews with nearly 150 technology, media and telecommunications organizations around the world.

This year's research has been part of a global, cross-industry program which has provided new and valuable insights about security in the TMT industry as compared with other industries.

Senior professionals in Deloitte's Information & Technology Risk Services practice conducted focused discussions with information technology executives of leading global technology, media and telecommunications organizations. Discussions focused on key aspects of strategic and operational areas of security and privacy across all industries. This report presents the analyzed and consolidated responses of the participants in both qualitative and quantitative formats.

The 2009 study found that investments in security had declined for many technology, media and telecommunications organizations as a result of wide-scale cost-cutting precipitated by the economic downturn. Spending levels shrank despite a marked deterioration in the enterprise security environment, the rising use of social networks in the enterprise, increased regulations, and the continued growth of outsourcing.

In 2010, spending on security appears to be bouncing back—albeit modestly—in anticipation of renewed economic growth. The key question is whether these relatively small budget increases will make up for the ground lost during the recession.

One encouraging sign is that technology, media and telecommunications organizations increasingly recognize information security as a strategic business issue and no longer just an information technology (IT) issue. On an even broader level, countries around the world are taking measures to counter the growing security threat from professional criminal and terrorist organizations engaging in cyber crime and cyber warfare.

An organization's information security can only be as strong as its weakest link. And as in previous years, employees and internal threats remain a significant problem that is often overlooked due to the focus on external threats. Similarly, business partners and other third parties are a growing concern as technology, media and telecommunications organizations increasingly operate as extended enterprises.

On a positive note, robust security capabilities are helping some organizations capitalize on bargains in the mergers and acquisitions (M&A) market, thus improving their overall business agility. Organizations are also raising the priority of protecting their digital assets, and are deploying new technologies and contractual agreements to build trust among customers and business partners and to minimize online fraud.

No report on information security would be complete without a discussion about one of today's hottest trends, cloud computing, which is expected to fundamentally change the way IT services are managed and delivered. But before cloud computing can become mainstream and attain its full potential, significant security and privacy issues need to be addressed.

On behalf of Deloitte Touche Tohmatsu (DTT) and the TMT practices of its member firms, we would like to thank all those who contributed to this report, especially the chief information security officers and security management teams that shared their experiences and insights. Your contributions are helping to make the technology, media and telecommunications industries more secure, and, as a result, more successful.



**Jolyon Barker**  
Global Managing Partner  
Technology, Media & Telecommunications



**Jacques Buith**  
Information Technology and Risk Leader



# 1. On the rebound

As the global economy prepares for renewed growth, technology, media and telecommunications organizations are starting to re-invest in information security.

At the time of the 2009 Global Security Study, the economy was in the deepest depths of a global recession and organizations were reviewing and cutting costs everywhere they could—including security. The damage done by last year’s budget cuts is reflected this year in respondents’ responses: 57 percent of organizations polled believe they are falling behind or still catching up in dealing with security threats. Only one-third of the respondents believe they are “on plan”—compared with 60 percent in the 2009 study.

This year’s study shows a slight increase in security investment in anticipation of an economic recovery. After more than a year of restricted spending and postponed projects, significant security and

infrastructure upgrades are finally underway. Many technology, media and telecommunications businesses were among the first to be affected by the economic crisis and are now among the first to benefit as economies recover. Technology organizations in particular are at the forefront of the recovery.

The study shows a noteworthy increase in information security budgets over the past 12 months. Ten percent of respondents increased their budget by more than 10 percent. Thirty-six percent increased their budget by up to 10 percent.

There was also a considerable decline in the proportion of organizations reducing their information security budget, which dropped from 32 percent in 2009 to 23 percent this year.

However, respondents still view inadequate security budgets as the biggest barrier to information security, with 46 percent rating budget as their number one issue.

**Figure 1: Characterize the year-over-year trend in your information security budget**

	Technology	Media	Telecommunications
Budget has been reduced	26%	36%	18%
Increase of 1% - 5%	24%	23%	35%
Increase of 6% - 10%	10%	9%	4%
Increase of 11% – 15%	0%	5%	6%
Increase of greater than 15%	6%	0%	14%
Not applicable / do not know	34%	27%	24%

Across all three TMT sub-sectors, media organizations were the most likely to be experiencing a declining budget for information security. They are also the organizations most likely to rate themselves as still catching up. Telecommunications organizations expected the largest year-over-year growth in security spending (see Figure 1). Overall, 20 percent of respondents from all industries faced budget reductions.

In light of the global recession—and still fragile recovery—38 percent of respondents have established metrics aligned with business value to measure the effectiveness of their security investments, while another 24 percent are moving in that direction. These figures show that technology, media and telecommunications organizations are trying to spend their information security budgets wisely. They want to obtain high security levels at a reasonable price and are positioning themselves for an optimistic (but still uncertain) future.



---

**Bottom line:** Although budgets are improving, they remain the greatest barrier to effective information security. This year's budget increases are a step in the right direction but may not make up for lost ground.

## 2. Clouds in the forecast

---

### Cloud computing could fundamentally change how IT services are delivered—but only if its security and privacy challenges can be resolved.

Cloud computing is receiving a lot of attention. Much of it is justified but in order for cloud computing to reach its full potential, it must overcome a number of major obstacles, particularly concerns over privacy and security.

One of the primary benefits of cloud computing is that businesses can gain access to the IT services they need without having to worry about all of the behind-the-scenes details. Those details are taken care of by the vendor. But when it comes to privacy and security, the details of how the service is managed and operates is critically important. After all, if a business doesn't have direct control over its systems and data, how can it be certain that everything is safe and secure?

#### What is cloud computing?

Cloud computing is a model that enables convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction.

Cloud computing includes five major defining qualities:

- On-demand self-service
- Ubiquitous network access
- Location independent resource pooling
- Rapid elasticity
- Pay per use

Examples of consumer cloud computing applications include Web-based email, Google applications and social networks.

Most technology, media and telecommunications organizations we studied (62 percent) are confident they can protect themselves from external security threats, compared with 64 percent in other industries. However, they are significantly less confident about the security and privacy threats caused by third parties they work with. This is a problem for cloud as organizations implicitly rely on third parties to provide infrastructure, applications and data hosting out of the cloud.

Data privacy is one of the key issues of cloud computing, particularly where confidential data or commercially sensitive intellectual property are involved. In fact, there are often laws that require an organization to maintain direct control over its data, or that prohibit data from being stored or handled in a different country. For example, the European Union (EU) Data Protection Act prohibits certain types of information from leaving the European Economic Area (EEA). Yet, with cloud computing in its purest form, the data is "in the cloud" and could be physically located anywhere on the planet.

At present, there are no generally accepted cloud computing standards with respect to assurance. This creates risk and uncertainty about the security and service quality that cloud vendors provide. It could also make cloud users more dependent on a particular vendor due to proprietary access protocols and programming interfaces. These new aspects require more than proper contract management alone and as such, organizations should investigate further into vendor lock-in, technology lock-in, business risks and IT risks.

Business continuity is another critical issue for software and infrastructure-as-a-service variants of cloud computing. Technology, media and telecommunications organizations' reliance on digital information and technology is already critical. Availability requirements of the cloud gain importance as multiple users and organizations make use of cloud services. Any disruptions may translate directly into lost customers and revenue.



In many industries, regulatory compliance is a key driver for investment in business continuity. But our study shows that in the TMT industry, only 18 percent of respondents see regulatory compliance as such (compared with 33 percent of respondents across all industries). However, technology, media and telecommunications organizations that either use or provide cloud-based services also face the issues of continuity and availability.

Robust contracts and due diligence are an important starting point for secure cloud computing. But in many cases, organizations need to do more. That might mean taking a hands-on approach to cloud security or hiring a specialist organization to oversee security at a cloud vendor's data centre—even if doing so undermines some of the principles and benefits of cloud computing. As the ultimate step also assurance will be provided as-a-service out of the cloud. When addressing the privacy element in cloud computing, it is important to appoint an executive responsible for privacy. One-third of technology, media and telecommunications organizations polled currently lack a privacy executive. In the media sector, the numbers are even worse, with 65 percent of organizations not having appointed a privacy executive. Furthermore, 32 percent of technology, media and telecommunications organizations currently lack a formal program to monitor and manage key privacy initiatives.

---

**Bottom line: Cloud computing may, in many scenarios, be a more efficient way to deliver and manage IT services. But in order to reap the full benefits, technology, media and telecommunications organizations must find ways to address a number of important security and privacy challenges.**

# 3. Combating organized crime

---

## Information security is now an issue of national security.

Just a few years ago, it would have been hard to imagine the President of the United States focusing on information security. Back then, attacks were typically associated with kids experimenting with computers in their basements. The usual outcome was often little more than a stern reprimand.

Fast-forward to 2010 and U.S. President Barack Obama has made defense against cyber warfare a top national priority. The U.S. government and many others have appointed national cyber coordinators. NATO has set up the Cooperative Cyber Defence Centre of Excellence (CCDCOE).

This dramatic shift is being prompted by the growing professionalization of cyber criminals and cyber terrorists. Geeks showing off for their friends are no longer the main problem. In their place, sophisticated organizations with political, criminal and social agendas have become a major driving force behind information security threats. For example, the famous Mariposa botnet (a botnet or robot network is a term largely associated with malicious software), which infected more than 15 million computers around the world, was perpetrated by criminals with “limited computer skills” who downloaded the necessary software from the Internet for less than a thousand dollars. Fortunately, one of them was so unsophisticated that, by using his home computer for his activities, he led police right to his door.

“Cyber” has given rise to an entire underground economy in which criminals and terrorists can buy not only credit card numbers but also malicious software and networks (such as botnets) and tools to launch denial-of-service attacks. Technology, media and telecommunications organizations find themselves stuck in the middle of this, both as high-profile targets and as the infrastructure and service providers that enable cyber crime and cyber warfare. Furthermore, telecommunications organizations are at the heart of every nation’s vital infrastructure, providing communications and connectivity supported by hardware from the technology manufacturers. Because national security increasingly depends on the TMT industry, it is no surprise that national intelligence agencies specifically look at, and continually review, their position toward technology, media and telecommunications organizations.

Almost one-third (30 percent) of organizations polled across all industries regarded the increasing sophistication of threats as a major barrier to ensuring effective information security (see Figure 2). Technology, media and telecommunications organizations perceive this as a greater barrier relative to other industries (a 7 percent difference) and with good reason. Technology organizations watch helplessly as their devices are used for cyber crime or cyber terrorism; telecommunications operators see their networks being used illicitly and their customers enticed by botnets; media organizations face the risk of blackmail, with criminals threatening to bring down their online channels unless paid.

**Figure 2: Top three major barriers that your organization faces in ensuring information security**

Major barriers organizations face in ensuring information security	TMT	All
Lack of sufficient budget	46%	28%
Increasing sophistication of threats	37%	30%
Emerging technologies	27%	19%

These threats to technology, media and telecommunications organizations and infrastructure affect the entire society. Imagine what would happen if the phone system or Internet were suddenly unavailable or if private and confidential information was exposed to the whole world. Technology, media and telecommunications organizations, in close cooperation with governments, must find ways to counter these growing threats. If they do not, they put themselves –and our modern way of life–in jeopardy.



---

Bottom line: The past decade has produced fascinating but chilling developments in information security and cyber warfare—and no one is immune. Technology, media and telecommunications organizations are at ground zero and need to arm themselves for battle.

# 4. Security in mergers and acquisitions

---

The right approach to information security can improve business agility.

The global recession and uncertain economic conditions have created a buyer's market for mergers and acquisitions (M&A). Lowered market valuations provide an opportunity for stronger technology, media and telecommunications organizations to acquire struggling businesses and niche market offerings at significantly reduced costs.

In the media sector, organizations in digital media and interactive gaming might be attractive acquisition targets for traditional media organizations making strategic shifts to online business models. In the technology sector, there is a continued drive to acquire specialized skill sets and the next wave of innovation, whether in services, applications or data storage/management. In the telecommunications sector, a primary focus is to expand and consolidate the industry footprint across both mature and developing territories—led by mobile and service offerings.

Every technology, media and telecommunications organization understands the need for financial due diligence when considering a merger or acquisition. But given the growing importance of data and information, there should also be a strong focus on IT and security. Most acquisitions include an entire IT environment that needs to be integrated and improved in order to achieve the same level of security, privacy and continuity that exists in the acquiring organization's current environment.



Top 3 areas of internal/external audit findings

1. Excessive access rights
2. Audit trails and logging issues
3. Lack of sufficient segregation of duties

Organizations that spin off a business also face a number of security challenges. Chief among them is how to prevent employees in the divested business from continuing to access the organization's systems and data. To that end, studied organizations rate identity and access management (IAM) as one of their top three security initiatives for 2010 both for the TMT industry and across all industries, up from number seven last year. In addition, 35 percent of respondents report that "excessive access rights" is the number one problem identified by internal and external security audits. Although IAM has traditionally played the role of gatekeeper, it is now also helping to improve

business agility and reduce IT complexity by enabling organizations to quickly control user access in the wake of an acquisition or divestiture.

In many situations, an organization's existing business partners are its most attractive acquisition targets. As noted earlier, half of the studied organizations are only "somewhat confident" or "not confident" about their business partners' information security practices—a fact that might make those partners less attractive as potential acquisitions. This is especially the case with most technology, media and telecommunications organizations because IT is their primary business process, whereas with other organizations IT generally supports the primary business processes.

---

**Bottom line: Information security should be a key focus of due diligence when considering a merger or acquisition. Acquiring a business with inadequate security capabilities and controls can expose an organization to unacceptable risks.**

# 5. Maintaining trust online

---

## Organizations need to protect their digital assets in a world where thieves and cheats are just a click away.

Technology, media and telecommunications organizations are increasingly creating and distributing their content digitally, an approach that has proved lucrative for some but one that has also created new opportunities for piracy, cheating and abuse.

There is a lot of money circulating in today's online world. And wherever there is big money, there will be criminals looking to grab their share.

In this new environment, security is paramount. Over half of technology, media and telecommunications organizations studied had suffered at least one external breach during the past year. About one-third faced repeated breaches via malicious software originating from outside their organization—breaches that could undermine the integrity of their business model.

These trends explain why so many technology, media and telecommunications organizations are prioritizing the security of digital assets, which they sell and distribute online. According to our study, 84 percent of technology, media and telecommunications organizations now regard digitized information and content as a primary asset that falls within the mandate and scope of the information security executive.

Online games, for example, are not always properly secured. Manipulating game play and high scores is easily done, which makes them vulnerable to security attacks and cheating. Traditional methods of security are not sufficient in this new space. In online gambling, "bots" (Web robots) are the biggest threat. These sophisticated software programs emulate the behavior of human players and are also able to think and act much faster than any human ever could, thereby gaining an unfair advantage.



Similar technologies are being used to defraud online advertisers. Click farms, which are groups of people paid to click on ads, and robots are used to generate fraudulent traffic. This activity is difficult to detect since the clicks are actually occurring from random IP addresses (usually spoofed or forged). Traditional banner advertising (or banner advertisements) fall prey to inline frames (IF), HTML documents embedded inside the ad, which take the information the online advertiser has paid for. As online advertising gains market share and influence, the problem will only get worse.

To minimize the extent of online fraud, new software is being developed that detects the use of bots, click farms, cheat engines and other forms of online fraud.

Contracts are another key focus area for online business models. Many online business models are structured as “extended enterprises” that require a large number of contractual relationships. Yet, all too often, these relationships are hampered by a lack of clarity over digital rights ownership and intellectual property rights. By monitoring and improving how they manage contracts, technology, media and telecommunications organizations can strengthen their relationships, boost revenue and reduce risk.

The concept of trust needs an extra dimension in the online world: validation. Although digital business models usually need easy accessibility, they also require safeguards for privacy and property rights. Because digital revenue streams are by nature difficult to control, they require independent validation and reporting in order to prevent fraud and misuse. The good news is that much of this validation can be automated. Smart technology is available that continuously extracts, collects and analyzes online transaction data to provide early warnings about potential problems, helping to detect and prevent intentional and unintentional human errors and system failures. The maxim in the online value chain should be: Trust but validate.

With the growth and success of digital life have come many concerns relating to the security and integrity of the digital environment. Trust in digital and online services is becoming a key growth enabler—or inhibitor—for the digital economy. Some US\$167 billion in market volume (2012) could be at risk, approximately 1 percent of GDP for the EU-27, with market value related to content and advertising being most exposed.

‘Digital Confidence’, a report by Booz Hamilton, 2009, downloaded on April 20th 2010 from [http://www.lgi.com/pdf/080904Booz\\_english.pdf](http://www.lgi.com/pdf/080904Booz_english.pdf)

---

**Bottom line: Building and maintaining trust in an online world can be a real challenge. It is hard to know if the people you are dealing with are trustworthy when they may not even be real people.**

# 6. Nature versus nurture

---

External attacks get most of the headlines but internal security risks are just as onerous.

People sometimes make mistakes and do things they aren't supposed to. After all, they're only human. Technology, media and telecommunications organizations should focus more on the human facet of security, specifically internal vulnerabilities.

The challenge of internal security is greater than ever, thanks to mobile devices, wireless networking and social media. Nowadays, most employees are equipped with a laptop and smart phone and are able to work and access the Internet from almost anywhere. Unfortunately, technological advancement and the new behaviors these enable, such as working in public spaces, have generally outpaced employee awareness of the risks of working remotely.

It is all too easy for employees to release sensitive business information without realizing the consequences of their actions. Potential problems range from losing a laptop to inadvertently sharing sensitive information while using social media.



According to our study, technology, media and telecommunications organizations are increasingly confident in their ability to handle these internal challenges. This year, 34 percent of respondents categorize themselves as “very confident” or “extremely confident” with regard to internal threats, up from 28 percent in 2009. Yet many technology, media and telecommunications organizations still lack confidence in their internal security practices. Half of the technology, media and telecommunications organizations studied experienced at least one internal security breach during the past year; 27 percent of TMT industry respondents believe their information security professionals are missing competencies to handle existing and foreseeable security requirements, compared with 24 percent across all industries.

Technology, media and telecommunications organizations are trying to address the problem through training and development. In fact, information security awareness and training is among the top three security initiatives for the coming year as was the case in 2007 and 2008, and more than 60 percent of the studied technology, media and telecommunications organizations have organized training for employees to identify and report suspicious activities, compared with 54 percent across all other industries. However, executives at most technology, media and telecommunications organizations do not receive customized security training, which might limit their ability to serve as role models for security awareness.

Most security awareness programs start with an e-learning module, which raises awareness and knowledge, but does not necessarily alter behavior. More extensive training will likely be needed to address more serious threats such as social engineering, which take advantage of human nature and reflexive behaviors.

In addition to training, other techniques and methods such as data protection must be deployed to help reduce dependency on human judgment and ensure a high level of security. In this year’s study, data protection ranks among the top five security initiatives undertaken by technology, media and telecommunications organizations. It is a major undertaking. Classifying existing information to identify what information needs to be protected from whom and to what level is the most time-consuming part of the exercise. But as daunting as the project may be, organizations now seem to recognize its importance.

---

**Bottom line: Internal security risks and human error can never be entirely eliminated. But with the right combination of training and data protection, they can be reduced to manageable levels.**

# 7. Weak links

---

## Information security problems in your value chain are your problems, too.

Today, very few businesses are entirely self-contained. Most rely heavily on supply-chain partners and other third parties for key business activities. Ensuring security across this highly distributed value chain is much more challenging than ensuring security within an organization's own four walls.

Managing an external business partner presents a different set of security requirements than managing an internal department. According to our study, the most common approach for ensuring security with third parties is "signing confidentiality and non-disclosure agreements" (69 percent). The other most common approaches are "contracts" and "controlling access of the third party to systems and data."

Effective security requires more than agreements and contracts. Given the increased importance of security and privacy, and the growing threat of attacks, many technology, media and telecommunications organizations are scrambling to ensure their business partners' security capabilities are up to date and verified. The study found that 44 percent of technology, media and telecommunications organizations have identified the security capabilities and controls of their business partners; however, only 22 percent have actually tested them. Twelve percent of technology, media and telecommunications organizations say they simply do not know what security capabilities and controls their partners have in place. In the current environment, this is no longer acceptable since it jeopardizes the continuity of every organization in the chain.

Despite the lack of testing and verification, 30 percent of technology, media and telecommunications organizations have "high confidence" in their third parties, and 42 percent are "somewhat confident." Only 8 percent are not confident. Perhaps this is proof of the popular saying that "ignorance is bliss."





Tighter security regulations could force technology, media and telecommunications organizations to take action on this issue. However, regulations alone might not be enough. Most rules and regulations are still based on physical business models rather than the online business models gaining prominence in the TMT industry. According to the study, 58 percent of respondents believe they receive adequate commitment and funding from senior executives to effectively address regulatory or legal requirements, compared with 53 percent globally. However, as was the case last year, most respondents believe regulatory requirements are at best “somewhat effective” for improving their information security.

Compared with organizations in other industries, technology, media and telecommunications organizations are more likely to handle security activities in-house. Outsourcing of security technology services in the TMT industry is on par with other industries but the use of external providers for business continuity and other security-related services is significantly lower.

---

**Bottom line: An organization’s information security is only as strong as its weakest link. To ensure a high level of security across the entire value chain, technology, media and telecommunications organizations cannot rely solely on agreements and contracts. They must take an active role in identifying and verifying that their partners’ capabilities and controls are up to the challenge.**

# 8. More than IT

## Information security is being recognized as a business issue, not just an IT issue.

More and more, technology, media and telecommunications organizations are recognizing that information security is integral to their business. Security is not just a matter of and for IT. Although information security executives most often report to the CIO (24 percent), a significant number (18 percent) report directly to the CEO. And a growing number report to the board of directors or COO. These numbers demonstrate the increasing importance of information security as a strategic business issue.

These reporting relationships are even clearer for business continuity management (BCM). According to the study, BCM executives most often report to the board of directors (14 percent), followed by the CEO and CFO. This is to be expected, as the overall scope of business continuity and disaster recovery is greater than for security. In fact, BCM is often the catalyst for aligning security with business values. BCM is especially critical for organizations that rely heavily on technology since they are the most at risk from system outages and service disruptions.

The frequency of reporting on security is also increasing at every level of business leadership (see Figure 3). At the board of directors, CEO, senior management and executive management levels, reporting frequency is up versus last year.

The frequency of reporting is about 50 percent higher in technology, media and telecommunications organizations than in other industries. Similarly, business involvement in defining security strategy is about 12 percent higher in technology, media and telecommunications organizations.

Figure 3: How often do you provide a report on the information security status or posture of the organization to the following positions?

	Monthly		Quarterly		Semi-annually	
	2010	2009	2010	2009	2010	2009
Board of directors	16% ▲	13%	18% ▲	11%	10% ▲	9%
CEO	22% ▲	20%	16% ▲	14%	12% ▲	9%
Senior and executive management	41% ▲	34%	17% ■	17%	8% ▲	5%

The need for improved information security and BCM is increasingly driven by customer requirements. In fact, customer requirements are now the second most important driver for BCM—a significant increase in importance compared with last year’s study and also a significant difference to other industries where the customer requirement doesn’t even rank among the top three drivers.

In the last 12 months, information security executives have focused more attention on governance and management issues (e.g., governance, strategy and planning, compliance and monitoring) and less attention on technical issues (e.g., assessment, consulting and architecture).

Overall, the level of collaboration between IT and the business is increasing, with 73 percent of respondents reporting that both sides helped to define the organization’s information security strategy. In many cases, the need for business continuity was the driving force.



---

**Bottom line: In the TMT industry, information security and business continuity are an integral part of the business. Reporting frequency and reporting relationships are changing to reflect that increased importance.**

# About the study

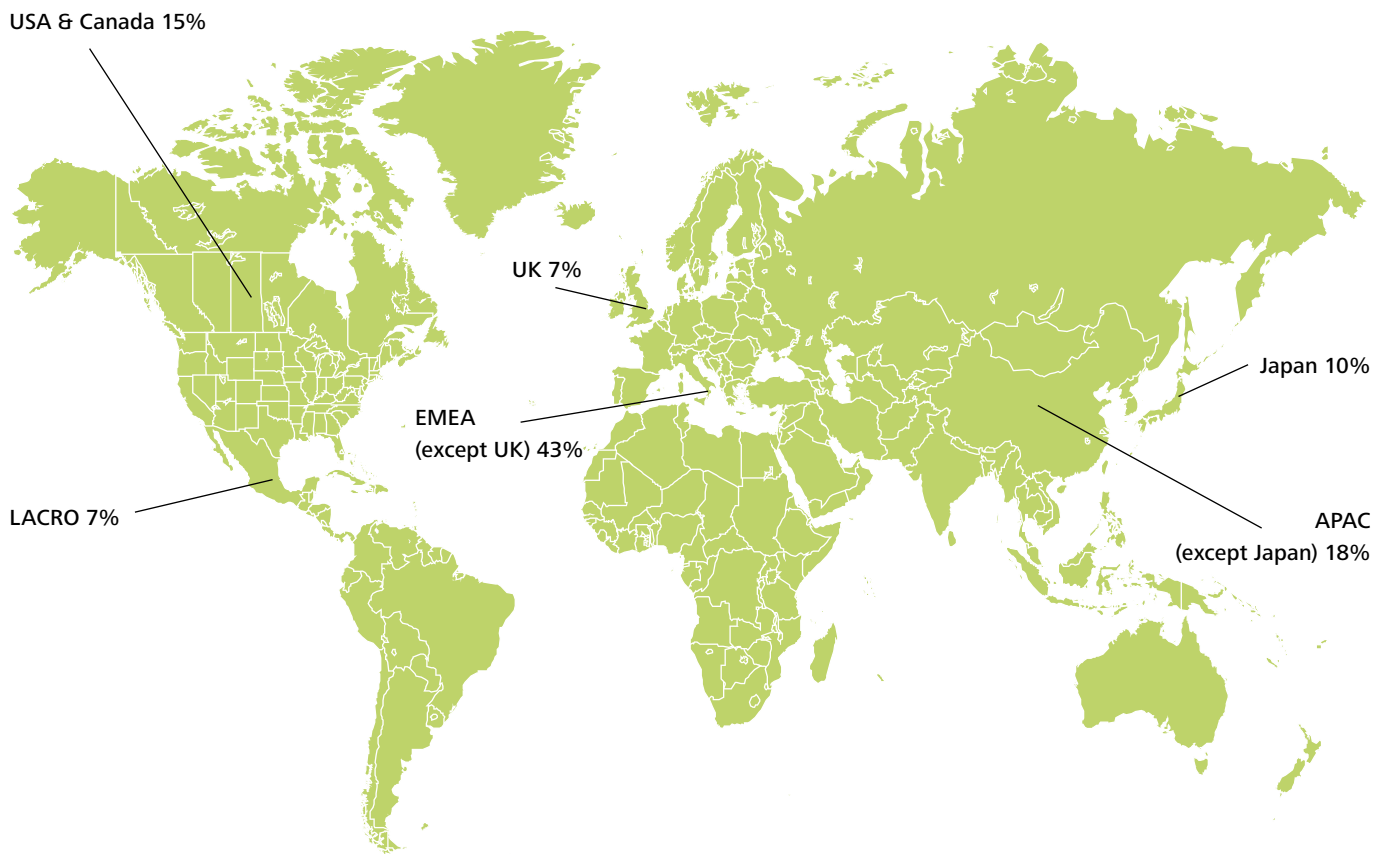
The responses in this study come directly from individuals working in the forefront of the global TMT industry. To encourage an open and honest dialogue, responses have been kept anonymous.

The findings are based on input from 146 technology, media and telecommunications organizations around

the world. Interviews were conducted by senior professionals from various member firm Information & Technology Risk practice.

## By region

TMT industry respondents came from 45 different countries representing every geographic region.



### By sector

Significant input was received from the TMT sectors.

Technology	35%
Media	15%
Telecommunications	50%

### By organization size

The study defined organization size as follows: “small” organizations having fewer than 1,000 employees; “medium” organizations having 1,000 to 10,000 employees; “large” organizations having more than 10,000 employees.

Small	31%
Medium	41%
Large	28%

### By revenue

Respondents spanned the full range of revenue categories (in USD).

<500M	23%
500M to 1B	12%
1B to 1.99B	15%
2B to 4.99B	15%
5B to 9.9B	9%
10B to 14.99B	2%
15B to 20B	4%
>20B	6%

# Acknowledgements

The Deloitte Touche Tohmatsu (DTT) TMT Industry Group wishes to thank all of the professionals of the technology, media and telecommunications organizations who responded to our study and who allowed us to further correspond with them over the course of this project. Without such participation and commitment, Deloitte Touche Tohmatsu member firms could not produce a study such as this.

## **Contributors**

The following made significant contributions to the development of this analysis:

### ***Jacques Buith***

+31 6 5585 3449  
jbuith@deloitte.nl

### ***Paul Lee***

+44 20 7303 0197  
paullee@deloitte.co.uk

### ***Hans Bootsma***

+31 6 1098 0182  
hbootsma@deloitte.nl

### ***Duncan Stewart***

+1 416 874 3536  
dunstewart@deloitte.ca

### ***Henk Marsman***

+31 6 2078 9905  
hmarsman@deloitte.nl

### ***Irfan Saif***

+1 408 704 4109  
isaif@deloitte.com

### ***Wouter Mocking***

+31 6 1234 2847  
wmocking@deloitte.nl

### ***Anneloes Leijenhorst***

+31 6 1004 2471  
aleijenhorst@deloitte.nl

# Contacts at Deloitte Touche Tohmatsu (DTT) and its member firms

## Global TMT

### *Jolyon Barker*

Global Managing Partner  
Deloitte Touche Tohmatsu  
Technology Media & Telecommunications  
Industry Group  
+44 20 7007 1818  
jrbarker@deloitte.co.uk

### *Igal Brightman*

Chairman  
Deloitte Touche Tohmatsu  
Technology Media & Telecommunications  
Industry Group  
+972 3 6085451  
ibrighman@deloitte.co.il

## TMT Information & Technology Risk Team

### *Adel Melek*

Canada  
+1 416 601 6524  
amelek@deloitte.ca

### *Ted DeZabala*

United States  
+1 212 436 2957  
tdezabala@deloitte.com

### *Uantchern Loh*

Malaysia  
+65 6216 3282  
uloh@deloitte.com

### *Martín Carmuega*

Argentina  
+54 11 4320 4003  
mccarmuega@deloitte.com.ar

### *Mitsuhiko Maruyama*

Japan  
+81 3 4218 7304  
Mitsuhiko.maruyama@tohmatsu.co.jp

### *Simon Owen*

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

## Local TMT Contacts

### Americas

#### *Alberto Lopez Carnabucci*

Argentina  
+54 11 4320 2735  
alopezcarnabucci@deloitte.com

#### *Marco Antonio Brandao Simurro*

Brazil  
+55 11 5186 1232  
mbrandao@deloitte.com

#### *John Ruffolo*

Canada  
+1 416 601 6684  
jrruffolo@deloitte.ca

#### *Fernando Gaziano*

Chile  
+56 2 729 8783  
fpgaziano@deloitte.com

#### *Nelson Valero Ortega*

Colombia  
+ 57(1) 546 1810  
nvalero@deloitte.com

#### *Carlos Gallegos Echeverria*

Costa Rica  
+506 2246 5000  
cagallegos@deloitte.com

#### *Ernesto Graber*

Ecuador  
+593 2 2 251319 ext. 246  
egraber@deloitte.com

#### *Francisco Silva*

Mexico  
+52 55 5080 6310  
fsilva@deloittemx.com

### *Cesar Chong*

Panama  
+507 303-4100  
cechong@deloitte.com

### *Gustavo Lopez Ameri*

Peru  
+51 1 211 8533  
glopezameri@deloitte.com

### *Phillip Asmundson*

United States, Deloitte LLP  
+1 203 708 4860  
pasmundson@deloitte.com

### *Juan José Cabrera*

Uruguay  
+598 2 916 0756  
jucabrera@deloitte.com

### *Johan Oliva*

Venezuela  
+58 212 206 8886  
joholiva@deloitte.com

## Europe, Middle East, and Africa

### *Nikolaus König*

Austria  
+43 1 537 00 7810  
nkoenig@deloitte.at

### *Andre Claes*

Belgium  
+32 2 600 6670  
aclaes@deloitte.com

### *Dariusz Nachyla*

Central Europe  
+48 22 511 0631  
dnachyla@deloittece.com

### *Olga Tabakova*

CIS and its Russian office  
+7 495 787 0600 x 2326  
otabakova@Deloitte.ru

**Kim Gerner**

Denmark  
+45 36 10 20 30  
kgerner@deloitte.dk

**Jussi Sairanen**

Finland  
+358 40 752 0082  
jussi.sairanen@deloitte.fi

**Etienne Jacquemin**

France  
+33 1 5561 2170  
ejacquemin@deloitte.fr

**Dieter Schlereth**

Germany  
+49 211 8772 2638  
dschlereth@deloitte.de

**Cormac Hughes**

Ireland  
+353 1 4172592  
cohughes@deloitte.ie

**Tal Chen**

Israel  
+972 3 608 5580  
talchen@deloitte.co.il

**Alberto Donato**

Italy  
+39 064 780 5595  
aldonato@deloitte.it

**Dan Arendt**

Luxembourg  
+352 451 452 621  
darendt@deloitte.lu

**Saba Sindaha**

Middle East  
+971 (2) 676 0606  
ssindaha@deloitte.com

**Anton Sandler**

Netherlands  
+31 88 288 0060  
asandler@deloitte.nl

**Halvor Moen**

Norway  
+47 23 27 97 85  
hmoen@deloitte.no

**Joao Luis Silva**

Portugal  
+351 210 427 635  
joaosilva@deloitte.pt

**Mark Casey**

South Africa  
+27 11 806 5205  
mcasey@deloitte.co.za

**Jesus Navarro**

Spain  
+34 91 514 5000 ext 2061  
jenavarro@deloitte.es

**Tommy Martensson**

Sweden  
+46850673130  
tommy.martensson@deloitte.se

**Oktay Aktolun**

Turkey  
+90 212 366 60 78  
oaktolun@deloitte.com

**Jolyon Barker**

United Kingdom  
+44 20 7007 1818  
jrbarker@deloitte.co.uk

**Asia Pacific****Damien Tampling**

Australia  
+61 2 9322 5890  
dtampling@deloitte.com.au

**William Chou**

China  
+86 10 8520 7102  
wilchou@deloitte.com.cn

**V. Srikumar**

India  
+91 80 6627 6106  
vsrikumar@deloitte.com

**Parlindungan Siahaan**

Indonesia  
+62 21 231 2879 ext 3300  
psiahaan@deloitte.com

**Yoshitaka Asaeda**

Japan  
+81 3 6213 3488  
yoshitaka.asaeda@tohatsu.co.jp

**Jum Pyo Kim**

Korea  
+82 2 6676 3130  
jumkim@deloitte.com

**Robert Tan**

Malaysia  
+603 7723 6598  
rtan@deloitte.com

**John Bell**

New Zealand  
+64 9 303 0853  
jobell@deloitte.co.nz

**Shariq Barmaky**

Singapore  
+65 6530 5508  
shbarmaky@deloitte.com

**Clark C. Chen**

Taiwan  
+886 2 2545 9988 ext 3065  
clarkcchen@deloitte.com.tw

**Marasri Kanjanataweewat**

Thailand  
+662 676 5700 ext 6067  
mkanjanataweewat@deloitte.com



---

“In 2010, spending on security appears to be bouncing back. However, the key question remains whether these relatively small budget increases will make up for the ground lost during the recession.”

Jacques Buith - TMT Information & Technology Risk Leader

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.

#### Deloitte Global Profile

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 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 169,000 professionals are committed to becoming the standard of excellence.

Deloitte's professionals are unified by a collaborative culture that fosters integrity, outstanding value to markets and clients, commitment to each other and strength from cultural diversity. They enjoy an environment of continuous learning, challenging experiences, and enriching career opportunities. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.

#### Disclaimer

This publication contains general information only, and none of Deloitte Touche Tohmatsu, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.