Deloitte.

Blurring the lines
2013 TMT Global Security Study

Contents

Information security in a world without boundaries

Foreword

Welcome to Deloitte Touche Tohmatsu Limited's sixth annual worldwide study report of information security practices in Technology, Media, and Telecommunications (TMT). Information security challenges continue to make headlines; in fact, it sometimes seems as if the bad guys are winning the battle.

To find out what businesses are doing to fight back, we surveyed executives from over 120 of the world's largest TMT companies. The results are both surprising and enlightening.

In last year's study, regulatory compliance was cited as the number one driver for improving information security. This year, compliance did not even make the top 10. Instead security strategy and roadmap top the list. This suggests that TMT organizations now recognize that information security is fundamental to their business, and not just a compliance issue anymore.

The big question is what to do next. TMT organizations face an onslaught of new and growing security threats, including *advanced persistent threats (APTs)* and *hacktivism*, the latter of which ironically combines destructive hacking with social and political activism.

At the same time, TMT organizations are trying to figure out how to manage new technologies such as mobile and cloud computing — technologies that promise to dramatically improve how businesses operate, but which also present significant new security challenges and risks.

Last but not least, TMT organizations must find ways to maintain and strengthen security in a hyper-connected world where third parties and digital supply chains are an integral part of their business models.

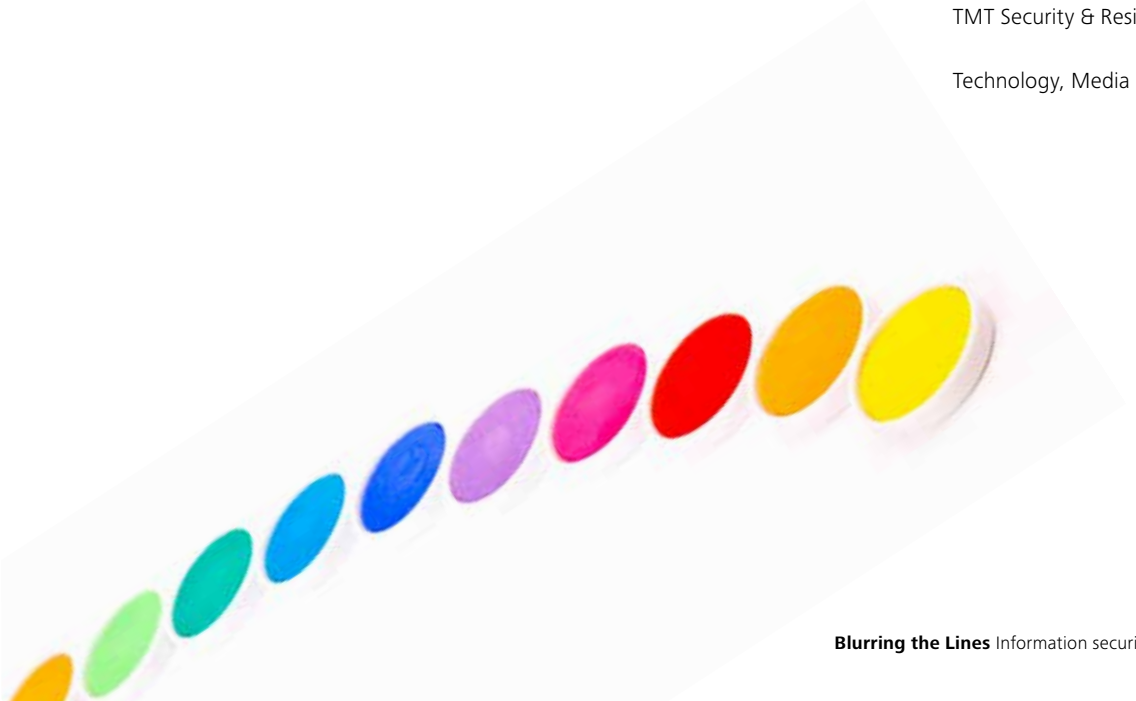
All of these trends are converging to create an environment where traditional security boundaries are blurry or even non-existent. How can a TMT organization build a strong way of defense against cyberattacks in a world without boundaries?

This report highlights the key information security challenges that TMT organizations face today, and offers a number of fresh and practical insights to help the good guys come out on top

Jolyon Barker
Global Managing Director

Jacques Buith
TMT Security & Resilience Leader

Technology, Media & Telecommunications



1. Investing in information security

Compliance is table stakes. Security is smart business.

Last year, security-related regulatory compliance was one of the top three security initiatives for TMT organizations. This year, compliance did not even make the top 10. Instead security strategy and roadmap top the list. The implication here is that TMT organizations now recognize how crucial information security is to their business success and are investing in it because it's smart business, not just because regulations require it.

Security is increasingly seen as a value-driver for the business and is becoming a significant differentiator in the marketplace. In addition, over 20% of our survey respondents indicate that information security is closely tied to critical business changes, such as business expansion, development of new services and products, organizational change, and (IT) strategy change.

The main question for TMT organizations today is how to achieve information security. According to this year's study results, the top security initiative for 2013 is to create a strategy and roadmap for information security. Organizations are taking a close look at their ever-increasing security threats, and then developing strategies and implementation plans to manage and mitigate the risks more effectively.

For TMT organizations with over 10,000 employees data leakage protection is also a top initiative — although there is significant variation between TMT sectors. Only 9% of Media organizations say they focus on data leakage protection, compared to 26% for Technology and 17% for Telecommunication. Media organizations focus more attention on end user awareness, as 27% of the Media respondents indicate. This goes for only 14% and 7% of respectively Technology and Telecommunications respondents. Respondents (19%) cited customer queries and complaints most often as the most important consequence of a security breach, indicating in many cases that information security is an integral part of the service provided by the TMT organizations. Customers today understand the importance of security and have little tolerance for mistakes. Strategies that seemed adequate in the past (such as conducting penetration tests once a year) are just not good enough anymore.

TMT organizations should look at information security in new ways that stretch beyond their own organizational boundaries. Also, they should actively market the fact that they are taking security seriously.

Information security and cyber risk have become boardroom priorities, as demonstrated by the World Economic Forum project, *Partnering for Cyber Resilience*. Also, the changing nature and posture of cyber risk make it an increasingly top-of-mind topic for TMT CEOs. That's one reason a growing number of CEOs support the Forum's project's *Principles for Cyber Resilience*[1].

In terms of specific threats, TMT organizations are most concerned about Denial of Service (DOS) attacks, which intentionally overload targeted systems and services, making them difficult or impossible to access. DOS attacks were rated as the highest threat by 28% of the survey respondents.

Top three security initiatives 2012

- Information security regulatory and legislative compliance
- Security related to technology advancements
- Information security training and awareness

Top three security initiatives 2013

- Information security strategy and roadmap
- Information security training and awareness
- Mobile security

1 See http://www.weforum.org/issues/partnering-cyber-resilience-pcr

Concerns about state/industrial espionage and malware that target industrial operating and *SCADA* environments vary widely by company size. According to our survey, these types of attacks are viewed as an "average" or "high" threat by 67% of large TMT organizations, but only 33% of smaller organizations (e.g. with less than 10.000 employees). This sizable gap suggests that large organizations may need to scrutinize the smaller organizations they work with to ensure sufficient countermeasures are in place. The level of concern also varies by industry sector, with 82% of Media organizations viewing these types of attacks as a "low" threat, whereas 50% of Technology organizations consider them a "high" or "average" threat.

One of the biggest obstacles to improving information security continues to be lack of budget. This was cited as a barrier by 49% of respondents. Although information security is increasingly important to TMT businesses — and the threats themselves are becoming more complex and numerous — security budgets have remained relatively flat. This is an issue that organizations will need to address if they want to stay a step ahead of the threats

49%

rate lack of budget the biggest barrier to improving information security

Deloitte bottom line: TMT organizations are now focusing on information security because their customers and the marketplace demand it, not just because regulations require it.

2. Dealing with external threats

Think you can't be hacked? Think again.

Many TMT organizations may be overconfident about their level of information security. In this year's study, 88% of all respondents (and 92% of Technology respondents) indicated they are "very confident" or "somewhat confident" that they are protected against external cyber threats. Also, more than 60% rate their ability to mitigate newly developed threats as "average" or "high." However, this widespread confidence may not be realistic.

Even the U.S. government's National Security Agency (NSA) works under the assumption that they have been compromised: "There's no such thing as 'secure' any more. The most sophisticated adversaries are going to go unnoticed on our networks. We have to build our systems on the assumption that adversaries will get in. We have to, again, assume that all the components of our system are not safe, and make sure we're adjusting accordingly"[2].

2 http://www.reuters.com/article/2010/12/16/us-cyber-usa-nsa-idUSTRE6BF6BZ20101216

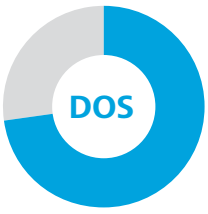
Among the TMT organizations surveyed, 68% believe they understand their cyber risks, and 62% say they have a program that sufficiently addresses these risks. Yet more than half knowingly experienced a security incident in the past year, and of those incidents, 7% were considered high impact. Other organizations may have had their security breached without even realizing it.

The truth is every organization is vulnerable; 100% prevention does not exist. That's why a combination of detection and incident response, in addition to prevention, is becoming more important. In fact, TMT organizations today are increasingly focusing on cyber resilience, not just security.

According to the surveyed organizations, network-related protective technologies (such as firewalls and network zones) are by far the most effective methods. Security compliance tools are considered the least effective.

Top three threats (perceived as high or average threat):

74%
Security breaches at third parties



73%
Denial of Service attacks

73%
Employee errors and omissions

Impact of the information security breaches in past 12 months:

59%
has had a breach

Percentage of respondents that had a breach

12% high impact
58% medium impact
30% low impact

Impact of breaches

A major threat that is relatively new is hacktivism, which combines social or political activism with hacking. Protesters who, in the past, might have blocked access to a business by staging a sit-in might now block access to its on-line operations through a DOS attack. Hacktivism can be triggered by any number of things, from potentially controversial business practices to saying or doing something that rubs a hacker group the wrong way — something that is very easy to do these days, thanks to social media and the internet. Whatever the trigger, once an organization has been targeted, the odds of it being effectively attacked are almost 100%. This has been clearly demonstrated by successful attacks which were very specific and targeted, such as *Aurora, Shady RAT, High Roller, and Stuxnet*. And those are just a few of the ones we know about. Unfortunately, the deck is stacked in the hackers' favor, as it takes a lot less effort to attack than to defend, there tends to be a lack of timely and accurate reporting about the nature of such attacks, and the chances of getting caught are very low. Effective handling of a hacktivist attack requires advance preparation, both from an IT and public relations perspective. Fortunately, our study shows that TMT organizations are starting to gather intelligence about these and other types of cyber crime incidents: 55% collect general information, and 39% receive information about attacks specifically targeted at their organization, industry, brand, or customers. Specialized companies can help gather this data, although that means having to deal with yet another third party.

Preparation is essential for other types of security challenges as well — especially business continuity and disaster recovery. Strong protection from external threats is not a substitute for business continuity management (BCM). Indeed, TMT organizations without robust BCM hardly can consider themselves ready to face the challenges of today's hostile business environment.

Deloitte bottom line: Prevention is an important first step; however, no organization can be 100% safe from attack. Robust detection and advance preparation and planning may help stop a breach from turning into a crisis.

3. People and technology

New technology risk is inevitable. People must learn how to handle it.

Technology advancements and the people using these technologies introduce information security risks. The human element is one of the biggest sources of information security risk identified by the respondents, as well as one of the most difficult to control. 70% of the TMT organizations surveyed rate their employees' lack of security awareness as an "average" or "high" vulnerability. Employees without sufficient awareness of security issues may put an organization at risk by talking about work, responding to phishing emails, letting unauthorized people inside the organization, or even selling intellectual property to other companies.

New technologies exacerbate the problem. Although they provide powerful new capabilities that may benefit the business, they also introduce new security risks at a faster pace than many organizations can handle.

According to this year's study, two technologies in particular have spawned associated trends that are creating significant security headaches:

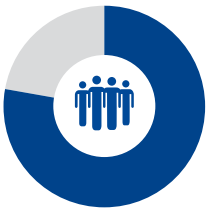
- The "Bring Your Own Device" (BYOD) trend in Mobile
- The "Rogue IT" trend in Cloud Computing

Both of these technology trends make it hard to secure an organization's information boundaries because they extend and blur the lines of defense.

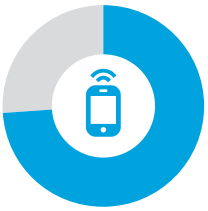
Mobile & Bring Your Own Device

Today's mobile devices enable employees to work anytime, anywhere, and are powerful enough to handle most business activities and data, including email, documents, contacts, and agendas. They are also used extensively for social media and access to cloud stored data. This intermingling of access to business data and use of personal software applications in one device makes mobile devices a prime target for hackers and provides new entry points for attack. Also, mobile devices are easily lost or stolen.

Top vulnerabilities (perceived as average or high threat)



78%
Number and type of third parties



74%
Increased usage of mobile devices

70%
Lack of sufficient awareness with employees

Last year's study participants were concerned about the mobile trend and feared it would be one of the biggest security threats in 2012. This year, their fears seem to have become a reality. TMT organizations now consider mobile devices to be their second biggest security risk, with 74% rating it as a "high" or "average" threat. According to respondents, this risk is surpassed only by the number of third parties they must deal with (79%).

The risks are even greater when employees use their own mobile devices, rather than sticking with the standard devices issued and managed by the IT department. According to the survey, for the TMT organizations with over 10.000 employees 64% indicates they have specific policies for mobile devices and BYOD. Yet, looking at the total pool of respondents, both large and small organizations, this percentage drops to 52% having such policies, and around 10% do not address BYOD risks at all.

Cloud Computing & Rogue IT

One third of the TMT organizations are already using cloud computing for critical and/or non-critical applications. Among those respondents, 39% of TMT organizations (yet within the Media sub-industry this is 61%) store critical data in the cloud. Yet many respondents acknowledge that with cloud there is no assurance of security whatsoever, and that ease of use often trumps security. In particular, it is often difficult to know where cloud data is physically stored and what national and local regulations apply to it.
Cloud also enables increasing occurrence of *rogue IT* by enabling individuals or groups within the business to easily gain access to software applications that are managed and controlled outside of the organization. In many cases, the internal people responsible for managing information security may not even learn about these rogue applications until their use is too extensive to control. What's more, cloud may increase an organization's vulnerability to third-party security risks.

The potential problems multiply when people use mobile devices to access cloud applications and to upload data to the cloud. These combined risks will only increase in the future as mobile and cloud technologies proliferate.

Privacy is another people-related challenge exacerbated by mobile and cloud. Yet, only 64% of TMT organizations currently have a privacy program in place. Large organizations seem to be doing better in this regard, with 80% having privacy programs in place. Telecommunications organizations are also doing better than their counterparts in other sectors, with 77% having privacy programs, and 57% having Chief Privacy Officers (CPO). Among our respondents in Technology and Media, less than half have a CPO.

Risk from new technologies is inevitable and constant. The best an organization can do is to create a resilient enterprise by preparing its people for the challenges that are likely to arise. That means raising employee awareness of potential security issues and risks, and training IT and security professionals how to handle the latest threats. Among the TMT organizations surveyed, 44% offer general security-related training to employees, and 30% offer targeted security training by job level. The most common certifications for security professionals are CISSP (47%) , CISA (36%), and CISM (37%). Media organizations trail in this area, with 36% indicating their security professionals have no certifications whatsoever. Also, security awareness is a stated priority for only 8% of large organizations, and for only 30% of small organizations, creating a clear opportunity for improvement.

3 Certification offered by ISC2.org
4 Certification offered by ISACA.org

Deloitte bottom line: People are part of the problem when it comes to information security, so they need to be part of the solution. Training and awareness may help TMT organizations manage the risks from new technologies.

4. Third-party security risk

A chain is only as strong as its weakest link.

In today's hyper-connected world of digital supply chains, outsourcing, and cloud computing, TMT organizations are more reliant than ever on third parties. No wonder TMT organizations consider third-party risks and vulnerabilities to be their biggest security threat.

Our previous studies show this issue has been a concern for quite some time; however, this year it rose to the top of the list, with 92% of respondents from organizations with over 10,000 employees rating security breaches at third parties as an "average" or "high" threat, and 79% of all respondents saying the sheer number of third parties they do business with is an "average" or "high" threat.

Working with other organizations can create significant business value, but it also creates significant risk. After all, a chain is only as strong as its weakest link. As businesses become more reliant on third parties — and as third parties develop their own downstream service networks and increasingly rely on cloud — TMT organizations are finding their data being shared and exposed in ways they don't understand or control. In this hyper-connected environment, a breach anywhere in the digital supply chain can undermine the information security of every organization involved.

Despite these rising challenges, many TMT organizations still mainly rely on contracts and similar methods as their primary weapons for managing third-party risk. Among the organizations surveyed, 88% require third parties to sign a confidentiality agreement, while 68% address information security issues in their contracts. That's fine. But what is the practical value of a contractual agreement when, as noted earlier, many organizations may be overconfident about their ability to fend off cyberattacks?

What TMT organizations should consider doing is to work with their third-party business partners to understand and improve their security practices and ensure their online businesses are resilient. Among our respondents, 67% make an effort to control third-party access to data, and 75% say they have identified third-party security capabilities, controls and organizational dependencies (although only 31% review and test them regularly). In addition, 31% have consciously tried to increase the cyber awareness of their suppliers and business partners (although 27% have done nothing of the sort). In the Telecommunications industry specifically 43% indicates they consciously try to increase awareness. This may be driven by audit findings, since Telecommunications respondents indicate that their the top audit findings are "business continuity" and "review of third-party connections."

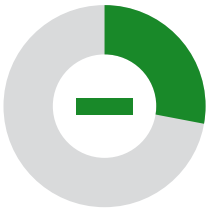
Hackers have built a loosely-coupled underground economy that helps them work together to launch attacks and steal secrets and money, more effectively than the above-ground economy. TMT organizations and their third parties need to fight fire with fire, collaborating in new ways based on trust and shared responsibilities, rather than relying on contracts and financial penalties. Key focus areas range from gathering intelligence and raising employee awareness to developing a robust security architecture that spans organizational boundaries

With whom outside of your organization do you raise cyber awarness?

31%
With our **suppliers** and **business partners**

29%
With our **customers**

19%
With **governmental** and **regulatory bodies**



27%
We **do not stimulate** cyber awarness

Deloitte bottom line: TMT organizations need to work with their third parties to understand and improve their combined security capabilities. Contracts alone are not enough.

5. Ready for action

Information security has become a top business priority. What's next?

Sharply reduced emphasis on security-related regulatory compliance, compared to last year, suggests that TMT organizations are now focusing on information security because it makes sense from a business perspective, and not just because government regulators require it. This is a watershed moment for the industry.

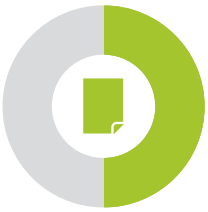
The question now is "what's next?" In a business environment where change is the only constant, traditional approaches to information security may not be enough.

The top security initiative for many TMT organizations is to develop a strategy and roadmap for information security that can help them tackle the growing list of threats. Unfortunately, many organizations seem to be over-estimating their current level of security, which may make them even more vulnerable to attack.

The cold, hard truth is that no organization is 100% safe from a security breach. Rather than place all of their bets on prevention, TMT organizations should consider investing significant time and effort into detection and response planning, with the goal of creating a resilient enterprise that can bounce back quickly from attacks. Cyber risk is fast becoming a top-of-mind priority for CEOs. Yet only 50% of the surveyed organizations currently have documented response plans in place. What's more, only 30% believe their third parties are shouldering enough responsibility for cybersecurity.

30%

Third parties are shouldering enough responsibility for **cybersecurity**



50%

Have **documented** response **plans** in place

In a hyper-connected world, collaboration with third parties is key, since a digital supply chain stretches an organization's information security boundaries beyond the range of its direct control. TMT organizations need to understand the security practices and risks for each of their third-party business partners, and then work side-by-side with those partners to address any problems and gaps.

Mobile and cloud technologies extend an organization's information security boundaries even further, almost to the point where boundaries cease to exist. In this increasingly open environment, technology-based security tools can only do so much. Ultimately, an organization's people must be part of the solution. Employees not being security professionals, need to be aware of information security risks so they can help mitigate them. In addition, IT security professionals need to be armed with the latest tools, techniques, and certifications so they can stay abreast of new developments and respond quickly when problems arise.

Last but not least, TMT organizations should engage in public-private collaboration by working with policymakers, regulators, and law enforcement agencies to address cyber risks. To some extent, this is already happening. For example, private sector organizations are often notified by law enforcement that a breach has occurred, and Telecommunications organizations frequently exchange information with the public sector about cyber threats and incidents. However, much deeper public-private collaboration is needed across all TMT sectors in a safe setting where organizations are willing to share their sensitive information.

Deloitte bottom line: The question is not if you will be attacked; the question is when — and how you will deal with it. Effective management of information security risks requires a robust combination of prevention, early detection, and rapid response that involves third-party business partners as well as the public sector.

About the study

The findings in this study are primarily based on in-depth, face-to-face interviews with 122 large TMT organizations around the world. Survey questions covered a wide range of topics on information security, from social media and mobile device technologies to training and information security governance.

By region

Survey participants came from 37 different countries representing every geographic region.

EMEA	70%
APAC	15%
USA and Canada	13%
LACRO	2%

By sector

There was significant participation from all three TMT sectors.

Telecommunications	47%
Media	21%
Technology	32%

By organization size

The study defined "small" organizations as having fewer than 1,000 employees; "medium" organizations as having 1,000 to 10,000 employees; and "large" organizations as having greater than 10,000 employees.

Small	35%
Medium	44%
Large	21%

By revenue

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

<500M	40%
500M to 1B	15%
1B to 1.99B	9%
2B to 4.99B	14%
5B to 9.9B	10%
10B to 14.99B	7%
15B to 20B	4%
>20B	2%

Partnering for Cyber Resilience – World Economic Forum

DTTL member firms are supporting the World Economic Forum on cyber risk management thought leadership, as the project advisor to the Forum's *'Partnering for Cyber Resilience'* initiative. In a series of interviews and workshops, senior professionals from DTTL member firms discussed the main topics in the Study and the most pressing issues in cyber risk management.

Acknowledgements

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

Contributors

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

Jacques Buith
Deloitte Netherlands
+31655853449
jbuith@deloitte.nl

Henk Marsman
Deloitte Netherlands
+31620789905
hmarsman@deloitte.nl

Adel Melek
Deloitte Canada
+14166016524
amelek@deloitte.ca

Roel van Rijsewijk
Deloitte Netherlands
+31652615087
rvanrijsewijk@deloitte.nl

Duncan Stewart
Deloitte Canada
+14168743536
dunstewart@deloitte.ca

Irfan Saif
Deloitte United States
+14087044109
isaif@deloitte.com

Peter van Nes
Deloitte Netherlands
+31610042150
pvannes@deloitte.nl

Maarten IJlstra
Deloitte Netherlands
+31613127325
mijlstra@deloitte.nl

Mike Lameree
Deloitte Netherlands
+31610999190
mlameree@deloitte.nl

Study execution

For more information on how DTTL's Global Technology, Media & Telecommunications Group designed, implemented and evaluated the study please refer to http://www.deloitte.com/tmtsecuritystudy.

Contacts at Deloitte Touche Tohmatsu Limited (DTTL) and its member firms

Global Security, Privacy & Resiliency
Ted DeZabala
Global Leader Security, Privacy & Resiliency
US National Leader, Technology Risk Services
+ 1 212 436 2957

Global TMT
Jolyon Barker
Managing Director, Global Technology, Media & Telecommunications
Deloitte Touche Tohmatsu Limited
+44 20 7007 1818
jrbarker@deloitte.co.uk

Security, Privacy & Resilience – Asia Pacific/Japan
Danny Lau
China
+852 2852 1015
danlau@deloitte.com

Security, Privacy & Resilience – EMEA
Mike Maddison
United Kingdom
+44 7768 554519
mmaddison@deloitte.co.uk

Security, Privacy & Resilience – US
Ted DeZabala
United States
+1 212-436-2957
tdezabala@deloitte.com

Security, Privacy & Resilience – Canada
Nick Galletto
Canada
+1 416-601-6734
ngalletto@deloitte.ca

Security, Privacy & Resilience – Latin America
Jose Gonzalez Saravia
Mexico
+52-55-50806722
jgonzalezsaravia@deloittemx.com

Americas
Alberto Lopez Carnabucci
Argentina
+54 11 4320 2735
alopezcarnabucci@deloitte.com

Marco Antonio Brandao Simurro
Brazil
+55 11 5186 1232
mbrandao@deloitte.com

Richard Lee
Canada
+1 416 874 3248
richlee@deloitte.ca

Fernando Gaziano
Chile
+56 2 729 8783
fpgaziano@deloitte.com

Nelson Valero Ortega
Colombia
+571 546 1810
nvalero@deloitte.com

Gilles Maury
Costa Rica
+506 2246 5000
gmaury@deloitte.com

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

Francisco Silva
Mexico
+52 55 5080 6310
fsilva@deloittemx.com

Domingo Latorraca
Panama
+507 303 4100
dlatorraca@deloitte.com

Johnnie Tirado
Peru
+51 1 211 8539
jotirado@deloitte.com

Eric Openshaw
United States
+7149131370
eopenshaw@deloitte.com

Adriana Berlingeri
Uruguay
+598 2 916 0756 x 6106
aberlingeri@deloitte.com

Johan Oliva
Venezuela
+58 212 206 8886
joholiva@deloitte.com

Europe, Middle East, and Africa
Luc Van Coppenolle
Belgium
+32 3 800 8905
lvancoppenolle@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

Jukka-Petteri Suortti
Finland
+358 20 755 5561
Jukka-Petteri.Suortti@deloitte.fi

Ariane Bucaille
France
+33 1 5561 6484
abucaille@deloitte.fr

Dieter Schlereth
Germany
+49 211 8772 2638
dschlereth@deloitte.de

Joan O'Connor
Ireland
+353 1 4172476
joconnor@deloitte.ie

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

Alberto Donato
Italy
+39 064 780 5595
adonato@deloitte.it

Nikhil Hira
Kenya
+254 204 230 377
nhira@deloitte.co.ke

George Kioes
Luxembourg
+352 451 452 532
gkioes@deloitte.lu

Dan Arendt
Luxembourg
+352 451 452 621
darendt@deloitte.lu

Daan Witteveen
Netherlands
+31 88 288 0236
DWitteveen@deloitte.nl

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

Joao Luis Silva
Portugal
+351 210 427 635
joaolsilva@deloitte.pt

Mark Casey
Southern Africa
+27 11 806 5205
mcasey@deloitte.co.za

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

Tommy Martensson
Sweden
+46 8 506 731 30
tommy.martensson@deloitte.se

Franco Monti
Switzerland
+41 44 421 6160
frmonti@deloitte.ch

Tolga Yaveroglu
Turkey
+90 212 366 6080
eroglu@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

Ichiro Nakayama
Japan
+09098044256
ichiro.nakayama@tohmatsu.co.jp

Sang Jin Park
Korea
+82 2 6676 3821
sjpark@deloitte.com

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

Ricky Lin
Taiwan
+886 3 5780899
rickylin@deloitte.com.tw

John Goeres
South East Asia
+65 6232 7118
jgoeres@deloitte.com

South East Asian countries

Daniel Fitzgerald
Guam
+671-988-4845
dafitzgerald@deloitte.com

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

Jimmy Lai
Malaysia
+603 7723 6541
jimmylai@deloitte.com

Luisito Amper
Philippines
+63 2 581 9028
lamper@deloitte.com

Shariq Barmaky
Singapore
+65 6530 5508
shbarmaky@deloitte.com

Weerapong Krisadawat
Thailand
+66 (0) 2676 5700
wkrisodawat@deloitte.com

Nam Hoang
Vietnam
+84 4 6288 3568
nhoang@deloitte.com

121120 2012