

# Treading Water.

The 2007 Technology, Media &  
Telecommunications Security Survey



# Contents

<b>Foreword</b>	<b>1</b>
<b>Introduction</b>	<b>2</b>
<b>Key findings of the survey</b>	<b>3</b>
<b>Detailed results</b>	<b>7</b>
Governance	7
Investment in information security	13
Risk	16
Use of security technology	23
Quality of operations	27
Privacy	30
Digital Rights Management (DRM)	34
<b>Design, implementation and evaluation of the survey</b>	<b>36</b>
<b>Contacts</b>	<b>38</b>
<b>About TMT</b>	<b>40</b>
<b>About the DTT ERS Security &amp; Privacy Group</b>	<b>40</b>

“TMT companies may be averting security crises, but are not getting in front of the problem.”

**Jacques Buith**

Security & Privacy Leader

Deloitte Touche Tohmatsu

Technology, Media & Telecommunications



# Foreword

Digital information and digital technology have had a huge impact on the world's economy, particularly in technology, media & telecommunications (TMT). In many respects this has had a positive impact that has driven significant revenue growth across the industry. However, it also presents TMT companies with a variety of new challenges and risks, including significant security threats.

For the second consecutive year, the Deloitte Touche Tohmatsu (DTT) TMT Industry Group, made up of the TMT practices of DTT member firms, conducted an in-depth survey of security practices at more than 100 TMT organizations around the world. Information was gathered primarily through face-to-face interviews with senior security executives.

Much has changed in the TMT industry over the past year; however, when it comes to security and privacy, the majority of TMT companies find themselves "treading water". Despite increased security investments, many are just managing to keep pace with the growing security and privacy threats. In order to get in front of the issue, TMT businesses should increase their security efforts and investments.

Those of us who specialize in security and privacy know that the answer to the question "Are we there yet?" is that we may never get there. Our job is to make the journey as safe and secure as possible.

This report looks at the latest security challenges and trends in the TMT industry, based on the views of those charged with securing TMT organizations, and offers specific and practical insights.

On behalf of DTT and the TMT practices of its member firms, we would like to thank all of the people who contributed to this report – especially the Chief Information Security Officers and security management teams of the participating companies that shared their experiences and insights. Your contributions are helping to make the entire TMT industry more secure.



**Igal Brightman**  
Global Managing Partner  
Deloitte Touche Tohmatsu  
Technology, Media & Telecommunications

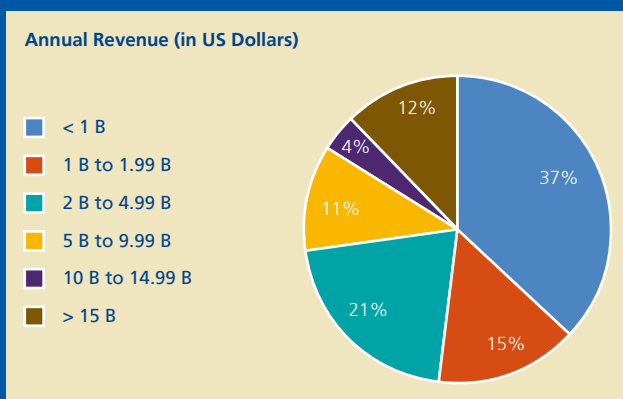
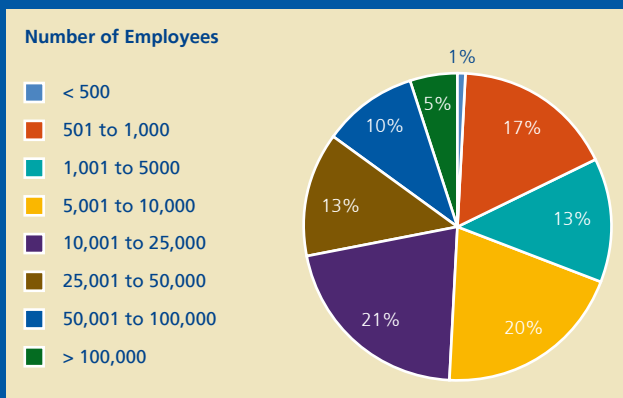
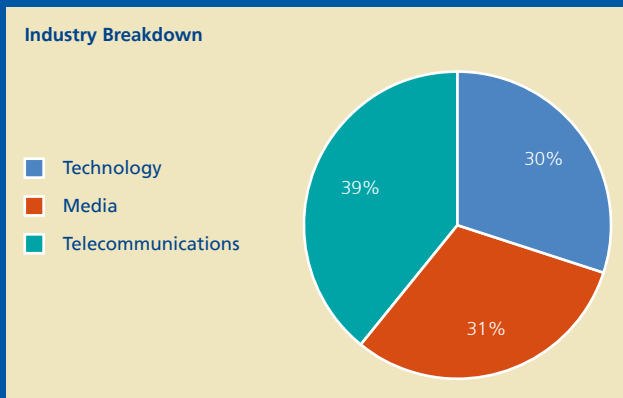


**Jacques Buith**  
Security & Privacy Leader  
Deloitte Touche Tohmatsu  
Technology, Media & Telecommunications

## Who responded?

The 2007 TMT Global Security Survey reflects current trends in security and privacy at more than 100 major global TMT companies. To encourage an open and honest dialogue around this sensitive subject, companies were invited to participate on the basis that their names would not be disclosed.

The global survey included organizations of varying sizes, with strong representation across all three sectors: technology, media and telecommunications. Among the participating companies, 54 percent employ between 5,001-50,000 employees, and 47 percent have reported revenue between US\$1 billion and US\$10 billion, meaning that the survey results are particularly relevant for large, global TMT companies.



# Introduction

## Objective of the survey

The first goal of the 2007 TMT Global Security Survey is to help TMT companies gain a better understanding of the security challenges and threats that the industry is already facing, and to provide insights to the challenges looming on the horizon. The second goal is to help TMT companies understand what others are doing to address the problem, so they can improve their own approach and reduce their vulnerability to attack.

This year's report builds on the results from the 2006 TMT Global Security Survey. Wherever possible, this year's survey questions have been kept the same as last year so as to help identify patterns and trends. In addition, the specialized knowledge and experience of DTT member firms were tapped to validate the survey results and provide new insights based on their hands-on experience with some of the world's leading TMT companies.

## The value of benchmarking

TMT companies recognize the importance of performance measurement and benchmarking – particularly in areas of the business that revolve around complex systems and processes. This survey was specifically designed to help TMT companies benchmark themselves against comparable organizations, allowing them to identify new and innovative practices that they can adopt and implement to improve their own performance.

## Areas covered by the survey

It is possible for an organization to excel in some areas related to information security (such as investment and responsiveness), while falling short in other areas (such as value and risk). To help TMT companies identify areas that require attention, the survey questions and analyses were grouped into seven categories:

- Governance
- Investment in information security
- Risk
- Use of security technologies
- Quality of operations
- Privacy
- Digital Rights Management (DRM)

# Key findings of the survey

## 1. Staying afloat

When it comes to security, the majority of the surveyed TMT companies have managed to keep their heads above water. In the 12 months preceding the survey, most responding companies successfully avoided a major security crisis. However, only a few increased their security capabilities to the point where they now feel as if they are ahead of the problem. According to the survey results, 49 percent of respondents are either falling behind or still catching up to the security threats. Only 7 percent believe they are ahead.

Although security investments generally climbed over the past year, the increases were often just enough to offset the rising volume and complexity of threats. Only a small number of the surveyed TMT companies (5 percent) increased their security investment by 15 percent or more. And half allocated less than 3 percent of their IT budget to security.

Moreover, only 38 percent of the surveyed companies believe their organization has all of the skills and capabilities they need to respond effectively and efficiently to security challenges.

On average, the number of security breaches was essentially unchanged from last year. This might seem like a small victory. After all, things could have gotten worse. However, organizations must adapt to the changing security landscape: the vulnerability of organizations will increase if they fail to keep up with the rising sophistication and complexity of threats.

**Bottom line:** TMT businesses should increase their security efforts and investments to address the problem. Companies that are not moving forward are likely falling behind.

## 2. Not yet business as usual

For TMT companies, digital information and digital technology have become business as usual. Unfortunately, the same cannot be said for information security – at least not yet.

The majority of business activities and assets in TMT revolve around ones and zeros: Online business models, digital content and distribution, databases filled with valuable information about customers and operations. The list grows longer every day.

Yet until there is a major problem, most companies do not spend nearly enough time and resources ensuring that their digital assets are secure, and often by then it is too late.

According to this year's survey, only 54 percent of the surveyed TMT companies have a formal strategy for information security, and only 14 percent say their information security strategy is led by the business.

**Bottom line:** In a digital world, information security needs to be business as usual – not something that only gets attention during a crisis.

### 3. More than an IT problem

Advances in information technology were a key driver for digitization in TMT, which more than likely explains why the IT function has traditionally been saddled with responsibility for information security. That approach might have made sense when digital information was a small niche. But now that digital content and digital distribution have moved to centre stage, it is time for business leaders to take charge of information security. IT can help tackle the problem, but the business needs to own it.

New online business models require an integrated security architecture from the very beginning. Those business models that incorporate security and foster trust and reliability have proven to be more successful than others.

According to this year's survey, 40 percent of the surveyed TMT companies still hold IT primarily responsible for information security. Moreover, only 62 percent currently believe that security is a key imperative at the board or executive level. That might not sound too bad, but the truth is security should be a top strategic priority for every TMT company – which means that percentage should really be much higher. In addition, 45 percent of respondents say top management is informed about security issues only on an ad hoc basis, or not at all. No wonder only 34 percent of the surveyed TMT companies believe that IT and the business are appropriately aligned on security initiatives. Given the increasing regulatory and legislative focus on information security and data protection, we would expect this number to be higher.

To make matters worse, 38 percent of respondents believe security is not a key imperative for business unit leaders. This is a real issue, because at most companies the business unit level is where strategy is converted from promising concepts into meaningful action.

A lack of executive support often translates into lack of funding. Only 55 percent of the surveyed companies believe they provide adequate commitment and funding for security initiatives, and only 38 percent have a budget for security separate from the IT budget. The funding problem is accentuated by the fact that the majority of the responding TMT companies (57 percent) do little or no measurement of security ROI. How can companies hope to justify their ongoing security investments if they make no attempt to quantify the returns?

*Bottom line: Information security is a business problem, not just an IT problem. Business leaders should take ownership of the issue and integrate it into their strategies and plans.*

### 4. The enemy within

When people think of security, they tend to focus on protecting the company from external threats. To that end, 69 percent of the respondents in this year's survey say they are "very confident" or "extremely confident" about their organization's effectiveness at tackling external security challenges. However, only 56 percent display a similar level of confidence toward internal challenges.

As last year's report demonstrated, the security threats from inside a company are just as great, if not greater, than the threats from outside. Deliberate fraud and misconduct are one aspect of the problem. But another critical aspect is simple human error. In this year's survey, 75 percent of respondents cite "human error" as one of the root causes for security failures – putting it at the top of the list, well ahead of operations (48 percent) and technology (48 percent).

One way to address the internal security challenges is to provide better training at all levels of the organization. Ongoing training helps people stay abreast of the latest threats and reminds them to remain vigilant. It also helps people avoid mistakes. Unfortunately, this is a weak spot for many TMT companies. According to the survey results, 42 percent of respondents have not provided employees with any training about security or privacy in the past 12 months.

*Bottom line: The most dangerous security threat comes from within. The good news? This is a threat that companies should be in a position to control.*

## 5. Protecting the customer

Companies today possess a vast amount of sensitive information about their customers: Purchase history, buying patterns and preferences, online behaviour, credit card numbers, and personal data. The loss or misuse of such information can have a devastating impact on customers, and expose a business to major lawsuits and other potential liabilities. It can also put a company at odds with privacy regulations, and cause immeasurable damage to a company's reputation and brand.

This is a serious problem, and it appears to be getting worse. News stories about the loss or theft of sensitive customer data are increasingly commonplace, and according to the survey, incidents that make the headlines are just the tip of the iceberg. Only 53 percent of the surveyed companies publicly disclose the loss of customer data, and many only do so in situations where disclosure is required by law.

Moreover, 36 percent of the companies in the survey do not track losses of customer data at all, and even fewer (32 percent) have performed an inventory of personal information. How can companies hope to protect something if they don't know what they have, or where it is?

Fortunately, many TMT companies are starting to focus significant attention in this area. Among our respondents, 33 percent have assigned a dedicated executive for privacy issues, and 72 percent have either just launched a privacy program (44 percent), or have an established privacy program in place and are launching key initiatives (28 percent).

**Bottom line:** Failure to protect customer information can expose the customer to a myriad of threats (such as identify theft) and expose the company to financial, regulatory and legal penalties.

## 6. The DRM dilemma

TMT companies are divided on the subject of digital rights management (DRM). Some see it as absolutely essential for protecting their content and other digital assets from theft and misuse; others see DRM as impractical and ineffective. Companies in the latter camp believe they can create more value for their customers – and their businesses – by investing in new products and features, rather than pouring time and money into DRM.

When discussing DRM as a concept, DRM supporters outnumber detractors by roughly 2 to 1. However, when evaluating DRM as an actual business strategy, survey respondents are evenly divided on whether DRM will be practical and useful within the next three years.

Over the past 12 months, there have been a number of high profile moves to eliminate DRM. The most widely publicized example was the challenge from Apple CEO Steve Jobs for music companies to abandon DRM. Shortly afterward, Apple's online music store began offering a significant number of songs without DRM; initially at a premium price, but now at no additional cost.

In this year's survey, 43 percent of respondents say they have identified IP loss / theft as a risk and put specific security measures in place. Roughly half of those companies (23 percent) are using some form of technology to protect their content.

**Bottom line:** When it comes to DRM, the only thing that seems certain is that the debate will not be ending any time soon.

## 7. Security beyond the four walls

More and more people are working outside of the office – at home, in their car, at a local coffeehouse, or wherever they can find space for a laptop, a signal for their mobile phone, and perhaps a high-speed internet connection. This trend is being driven by ongoing technology advances, and by a talent crunch that is prompting companies to give employees more latitude over when and where they work.

For many employees, the freedom to escape the confines of a traditional office setting is a dream come true. But for a company trying to maintain security in these highly unsecured environments, it can prove very challenging. The past year saw numerous highly publicized incidents where a lost or stolen laptop computer allowed unauthorized access to huge quantities of confidential data, and as advances in storage technology make it possible for people to carry even more data in a pocket or computer bag, the risks will only get bigger.

Introducing “end-to-end” security is a must for TMT organizations in order to stay ahead of the security challenges. End-to-end security starts with introducing information security policies that span the extended enterprise.

Another big challenge is that TMT companies are increasingly relying on outsiders – including strategic business partners, outsourcing vendors, and independent contractors – to help them deliver their products and services to the marketplace. In addition, 59 percent of the surveyed companies rely on other organizations for parts of their security function. To gain assurance, third party capabilities should be tested periodically; however, only 22 percent of respondents conduct such testing.

The extended enterprise model requires that a company pay close attention to the security of its mobile workers and the security capabilities of its business partners in order to ensure its digital assets remain protected across the entire value chain. After all, a company's security is only as strong as its weakest link.

*Bottom line: Information security risks extend beyond a company's four walls. With increased mobility and trends for outsourcing services, this is only going to increase. Companies need to start getting it under control now.*

## 8. Information security meets physical security

Today's TMT companies are built on a base of physical assets (e.g., buildings and infrastructure) and information assets (e.g., digital content). Yet most companies continue to treat physical security and information security as separate and distinct. In fact, the survey shows that 64 percent of TMT companies have done little or nothing to integrate the two, which means they could be missing out on some important opportunities.

For example, an access card or wireless chip normally used to control physical access could also be used to help prevent unauthorized information access. When someone tries to log on to an information system, the system could connect with the company's physical security systems to make sure the person associated with that user id is actually present in the building. If not, it could deny access and trigger a silent alarm.

This is just one example of how integrating physical security with information security could help to strengthen both. With TMT assets becoming increasingly information-based and virtual, the distinction between physical security and information security may soon be obsolete.

*Bottom line: In the future, companies may be able to improve their overall security by integrating virtual security with physical security.*

# Detailed results

## Governance

Information security is an important topic for TMT companies. Today's headlines are filled with stories about all kinds of security breaches: identity theft, data leakage, account fraud, phishing, and more.

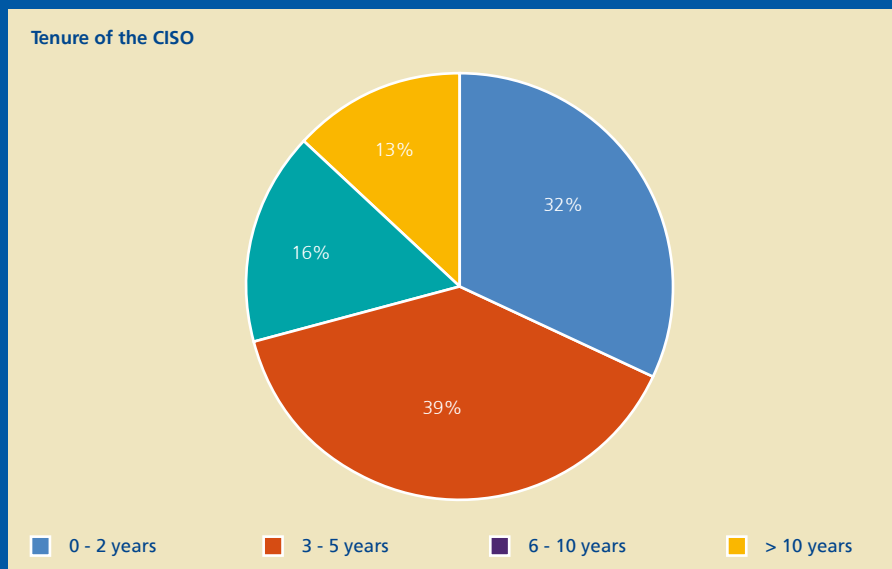
Managing these information security risks is a challenge. On the one hand, a company should do what it can to ensure that risks are being managed at acceptable levels. On the other hand, it also should recognize that a certain amount of risk-taking is fundamental to business growth and development. The trick is finding the right balance – and having the right governance can help.

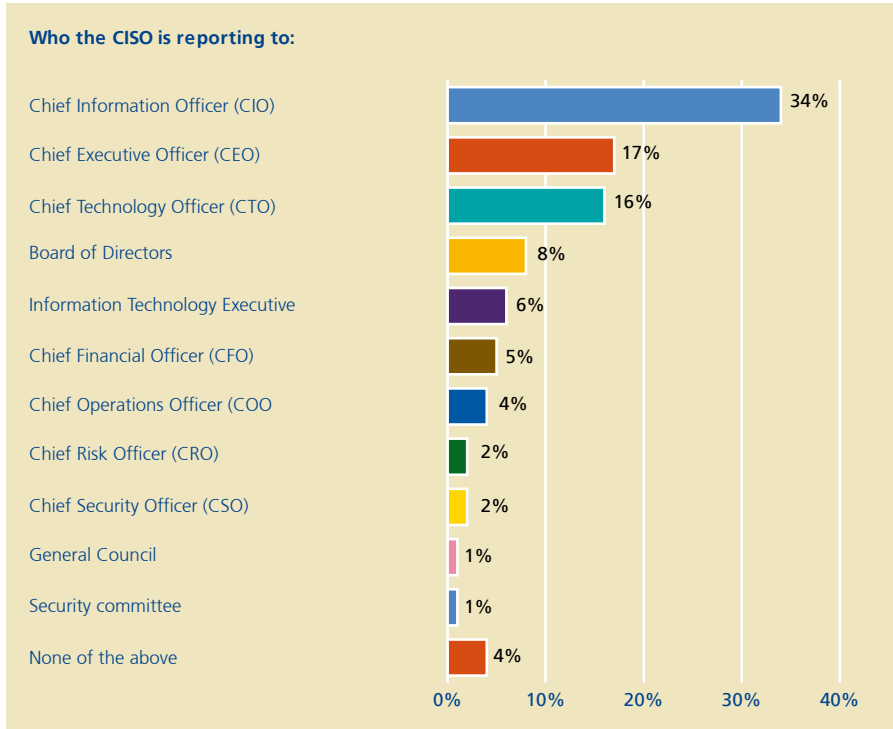
### Information security governance framework

A governance framework defines the roles and responsibilities, policies and procedures, guiding principles, and accountability requirements for managing information security. Most respondents (82 percent) already have such a framework, and another 12 percent plan to create one within the next two years. Only a few organizations (6 percent) don't have one, and don't intend to.

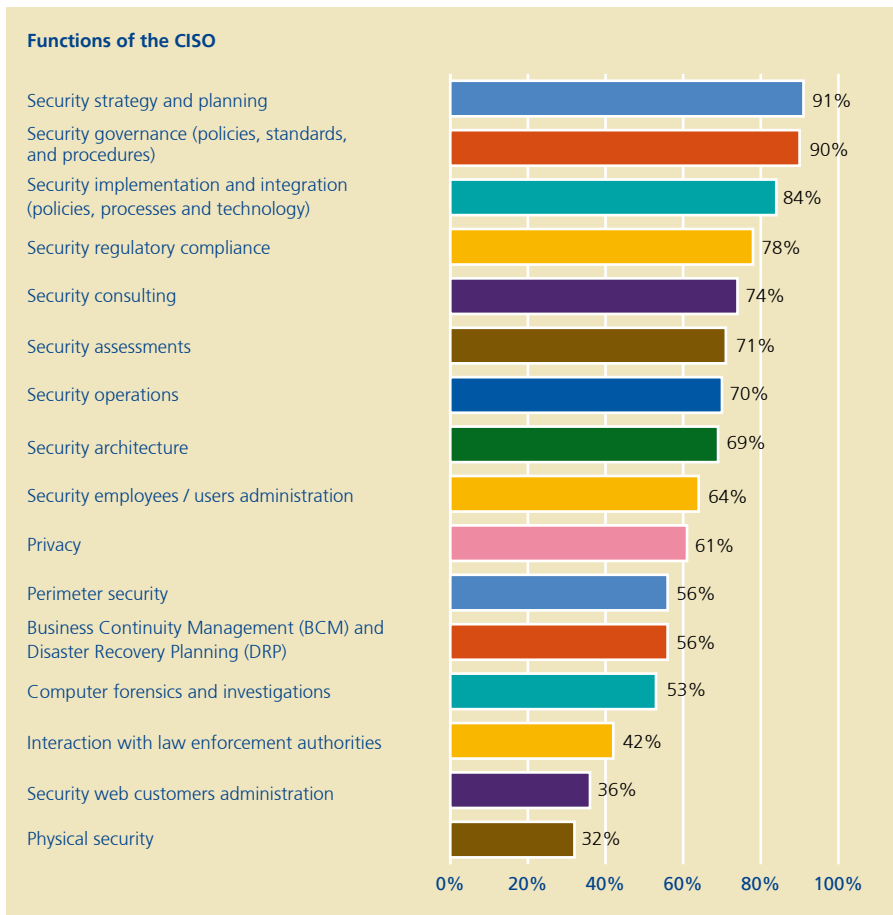
One of the keys to effective information governance is assigning a Chief Information Security Officer (CISO). Over the past year, the number of respondent organizations with a CISO (or equivalent) increased from 57 percent to 65 percent.

Most CISOs have been in their current position for less than five years:





According to the survey, the majority of CISOs (56 percent) report to someone in the IT organization (CIO, CTO, or IT executive). A smaller number report directly to the CEO (17 percent) or Board of Directors (8 percent).



CISOs have a wide range of responsibilities, the most common being security strategy and planning (91 percent), and security governance (90 percent).

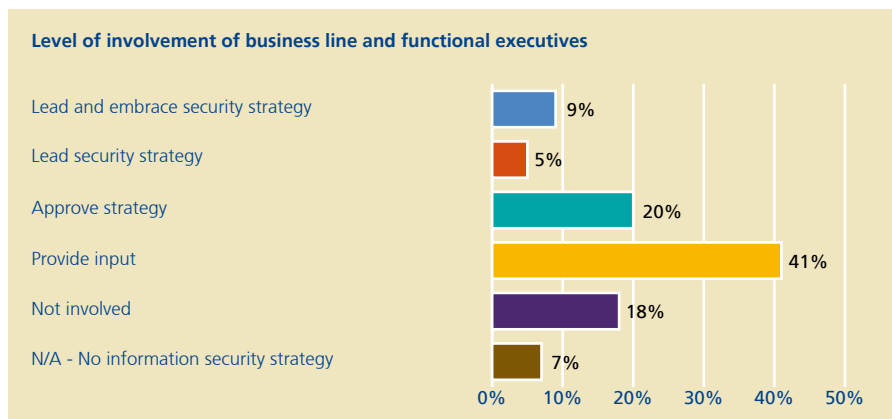
The information security function continues to grow steadily. Over the past 12 months, 54 percent of the surveyed companies increased their headcount in this area, while 40 percent stayed the same. Only 6 percent reduced headcount for information security.

The quest for qualified talent also continues unabated. In this year's survey, 35 percent of respondents say their organization is missing skills and competencies to handle existing and foreseeable security requirements. In addition, respondents rated "lack of resources" as the biggest barrier to delivering information security. To help address these challenges, 27 percent of the surveyed companies are supplementing their in-house capabilities through outsourcing and other non-traditional sourcing strategies.

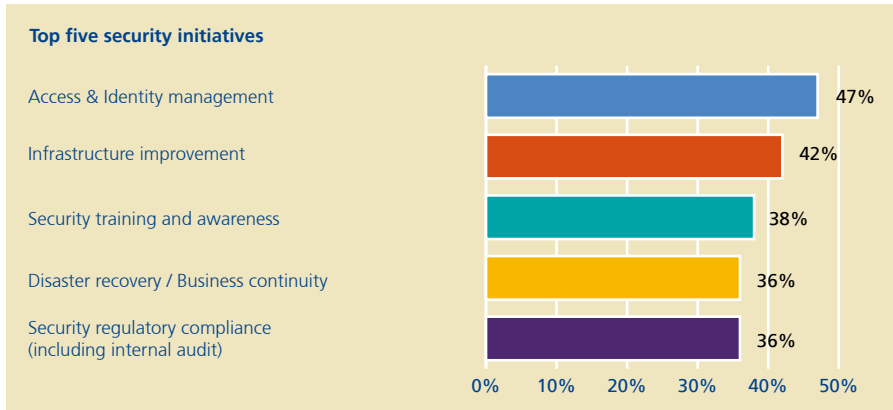
## Strategy

Another prerequisite for effective information security is the implementation of an information security strategy that aligns with corporate initiatives. Such a strategy should be closely linked to the company's overall business strategy, business requirements, and key business drivers. The survey results show that 54 percent of TMT companies have put a formal information security strategy in place. Another 20 percent intend to do so within 2 years. Moreover, 17 percent of the surveyed companies see the lack of such a strategy as one of their biggest barriers to achieving information security.

Only 34 percent of respondents indicate that business and IT security initiatives are appropriately aligned. Also, a significant number (18 percent) say that business line and functional executives have no involvement or input into the organization's information security strategy. Moreover, only 14 percent believe the business plays a lead role in information security.

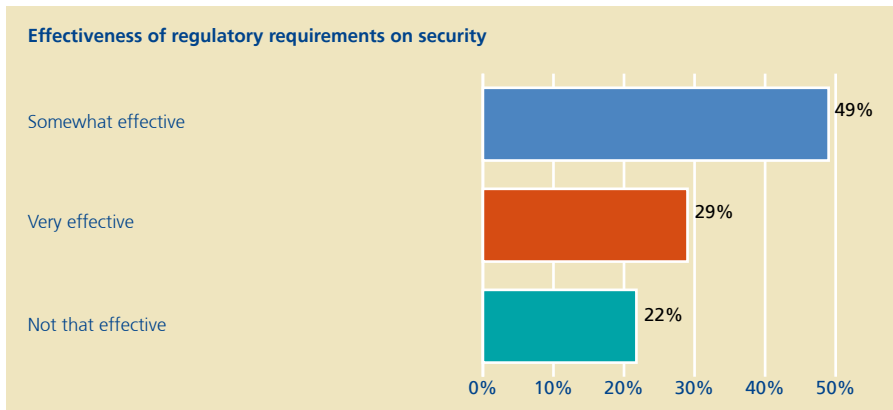


Respondents were asked to select their top five security initiatives for 2007. Surveyed companies rate "Access & Identity management" as this year's number one security initiative. "Infrastructure improvement" is a close second.



## Compliance

TMT companies face a growing number of rules and regulations related to information security. In principle, these regulatory requirements are designed to improve information security and reduce risk. According to the survey results, 29 percent of respondents believe that current rules and regulations are "very effective" in this regard, while 49 percent find them "somewhat effective". However, 22 percent rate them as "not that effective".



Among the surveyed companies, 12 percent are considering the adoption of international standards such as ISO 27001:2005 and plan to undergo certification within 12 months; 13 percent are in the information gathering stage; and 8 percent have either achieved BS7799-2:2002 certification or are in the process of transitioning to ISO 27001:2005.

## Measurement

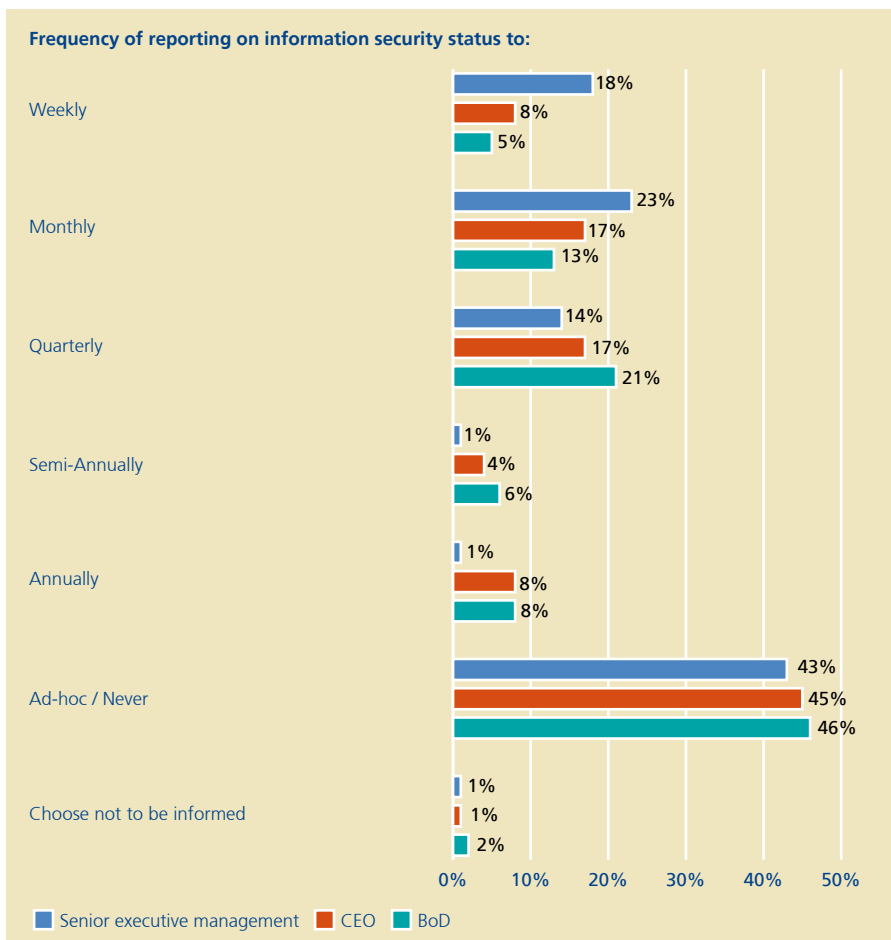
Reporting and measurement are considered the top initiatives for 2007 by almost a third of respondents (28 percent). In order to demonstrate effective information security governance, a company should understand and define its expected outcomes, performance targets, efficiency measures and related reporting requirements. Yet, according to the survey, only 19 percent have established formal metrics for information security.

- We have established formal metrics: 19%
- We are working on establishing formal metrics: 24%
- Little, if any, measurement is made of security ROI: 25%
- We do not measure: 32%

According to the survey, 41 percent of TMT companies consistently track and monitor the effectiveness of information security controls and have integrated reporting and measurement into their information security program. Another 34 percent are in the process of doing so.

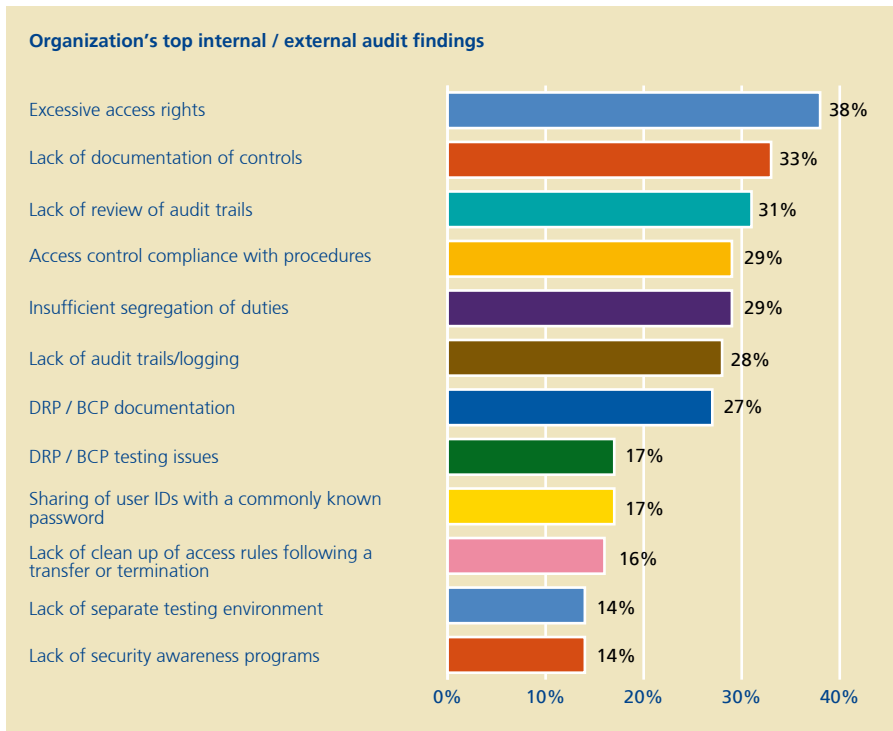
## Reporting

When asked about the frequency of reporting on information security, approximately 45 percent of our respondents say company leaders are provided with security reports only on an ad hoc basis, or not at all.



## Audit

Another key element in the governance framework is the performance of independent reviews and audits. When asked to identify their organization's top internal / external audit findings over the past 12 months, respondents cited the following:

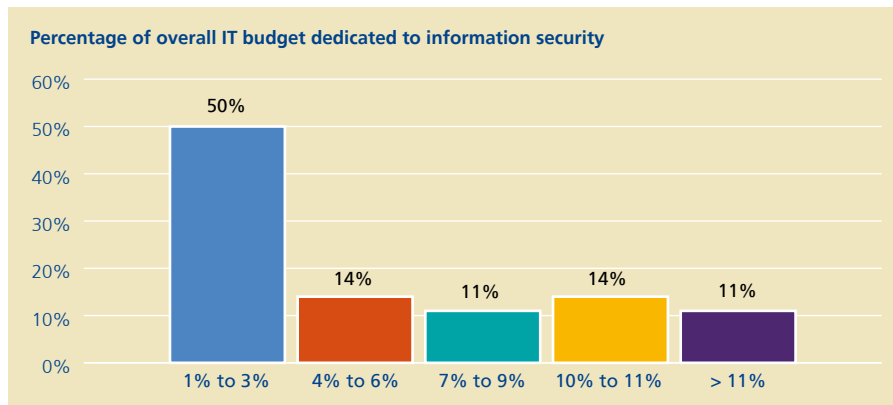


Three of the top 12 audit findings relate to access, which probably explains why “access and identity management” ranked as the top security initiative in this year’s survey.

## Investment in information security

Compared to last year, TMT companies' investment in security increased only slightly. Among the surveyed companies, 14 percent did not increase their information security budget at all, while 41 percent raised their budget less than 5 percent. Only 5 percent of TMT companies reported increases of more than 15 percent. As was the case with last year's survey, the DTT TMT Industry Group believes these minimal increases in security investment are barely enough to keep pace with the growing list of challenges, emerging technologies, and increasingly sophisticated attacks.

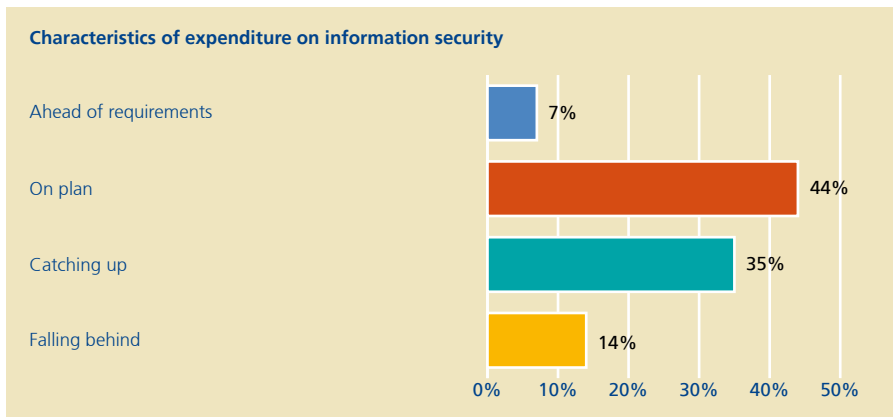
Moreover, the information security budget is often still lumped together with the IT budget. For 62 percent of respondents, the security budget is included in the IT budget, indicating that security is still perceived as an IT issue. Since security is becoming increasingly crucial for today's TMT businesses, it seems reasonable to expect that security would represent a large portion of the budget. Yet more than a majority of respondent TMT companies (64 percent) allocate less than 6 percent of their IT budget to information security, and half of the surveyed companies only allocate 1 to 3 percent.



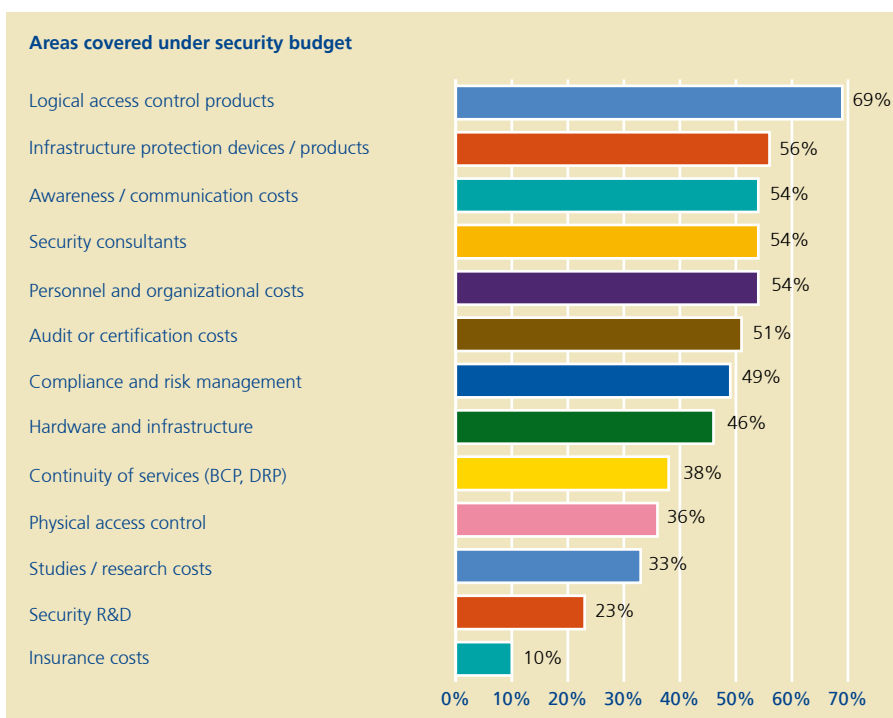
## Spending

An analysis of information security spending per capita provides deeper insight. The results show that 64 percent of the surveyed TMT companies spend at least US\$500 per employee on security. And 12 percent spend more than US\$1,000 per employee.

In last year's survey, 54 percent of TMT companies believed their security investments left them "falling behind" or at best "catching up" to the security problem. This year's results show a slight improvement, with 49 percent of respondents saying they are "falling behind" or still "catching up".

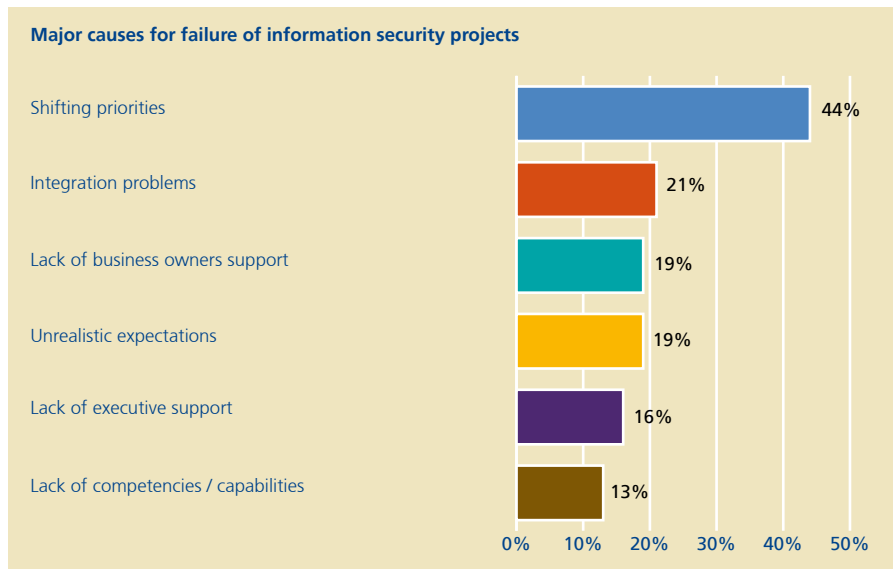


The survey results show "logical access control products" as the biggest focus for security spending, followed by "infrastructure protection devices". "Awareness and communication" are also relatively high on the list due to the fact that human error remains one of the primary causes of disruptions and security breaches.



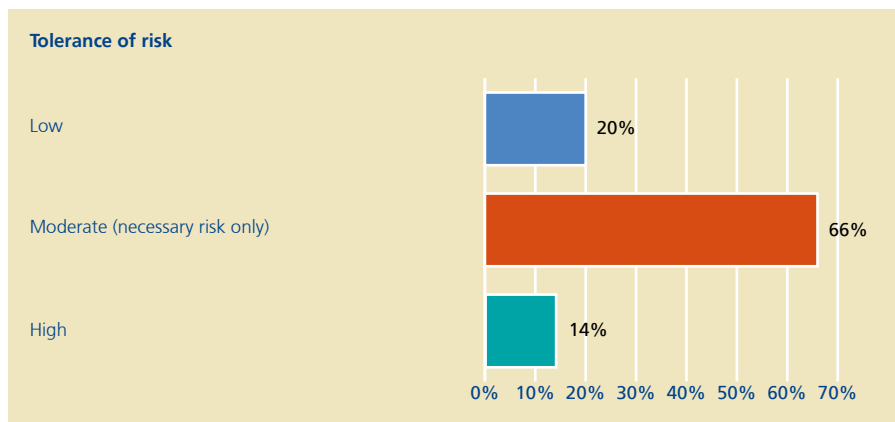
According to the survey, 36 percent of TMT companies do not measure whether their information security projects deliver what is expected or promised. Moreover, among the companies that do track this critical information, only 24 percent believe their information security projects deliver as promised.

Respondents were asked to select the major causes for failure of information security projects to deliver on promise. For projects that fail, the main cause appears to be “shifting priorities” (44 percent). This is followed by “integration problems” (21 percent), “lack of business support” (19 percent), and “unrealistic expectations” (also 19 percent). However, project failures may also be linked to the limited effectiveness of the information security function. The survey results show that 82 percent of respondents believe their information security function is at best “somewhat effective”. General improvement in this area might help TMT companies get more value from their information security projects.



## Risk

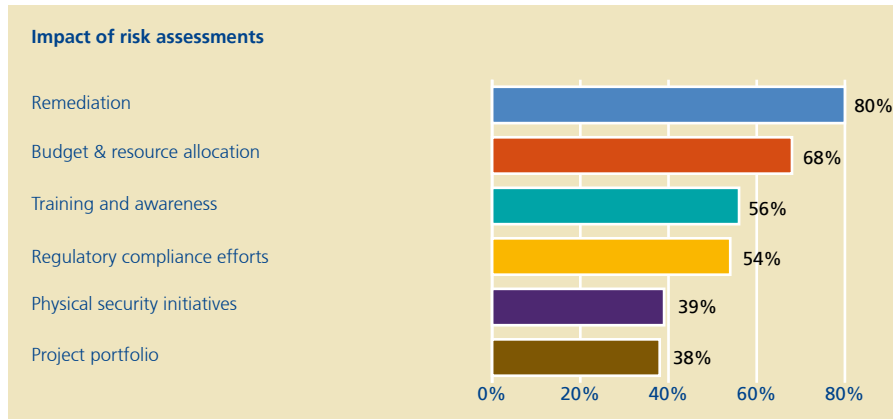
For TMT companies, IT and information security remain crucial for protecting the organizations' digital assets. In this year's survey, 66 percent of respondents indicate a "moderate" level of tolerance for risk (taking necessary risk only), 20 percent characterize their organization's tolerance for risk as "low", and 14 percent indicate a "high" risk tolerance.



Managing risk effectively and protecting the company from internal and external security breaches continue to be big challenges. Compared to last year, the number of security breaches was essentially unchanged. Among the surveyed companies, 26 percent saw an increase in security breaches, 30 percent saw a decrease, and 44 percent experienced no significant change.

Overall, TMT companies seem to be well on their way to establishing efficient risk management solutions. Among the respondents, 63 percent now classify their critical IT business assets by level of risk, and classify their information assets by level of confidentiality. However, this indicates that more than one third (37 percent) do not classify their critical IT and information assets.

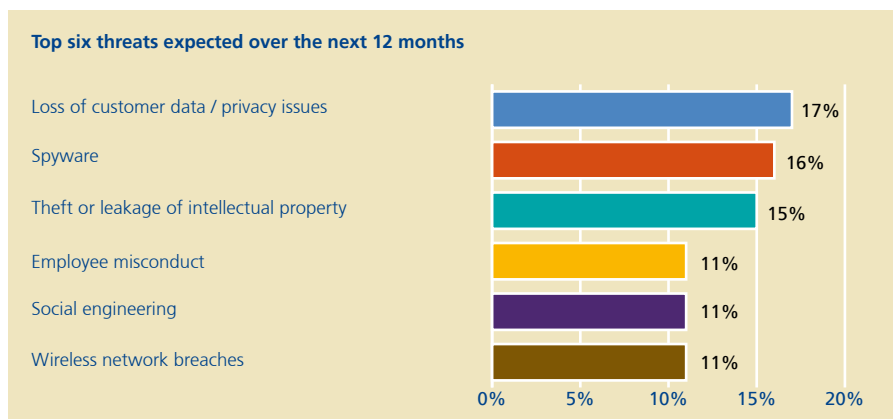
According to the survey, 75 percent of TMT companies identify, quantify, and prioritize risks against formal criteria and key operating objectives. To varying degrees, these risk assessments are used to support a wide variety of business decisions:



With regard to application security integration, 35 percent of respondents incorporate application security in the software development lifecycle, almost half (49 percent) say it varies from project to project, and 16 percent believe it is mostly an afterthought.

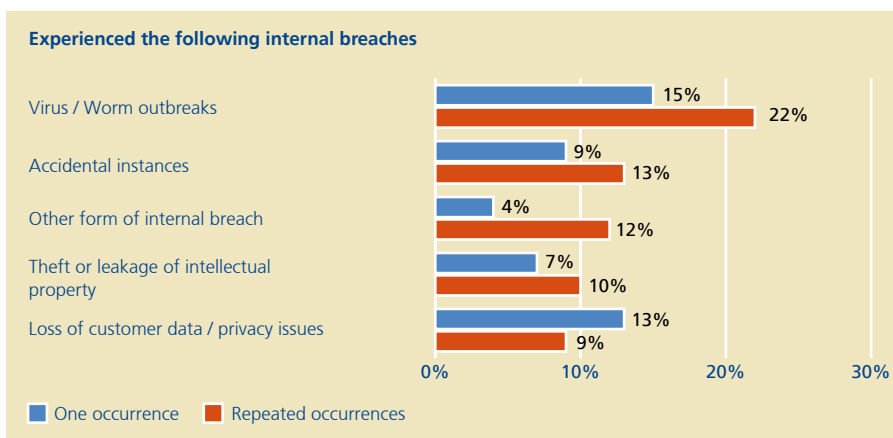
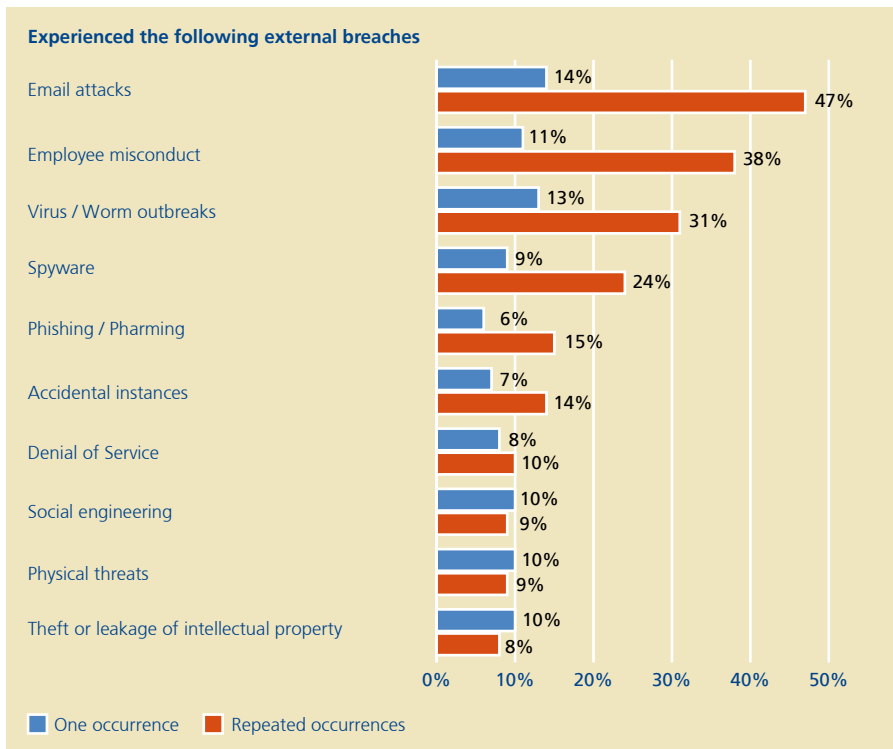
## Malicious external threats and operational threats

The survey provided a list of malicious external threats and operational threats and asked respondents to rate them on a scale from 0 (not a threat) to 5 (very high threat). The top six threats over the next 12 months are expected to be:

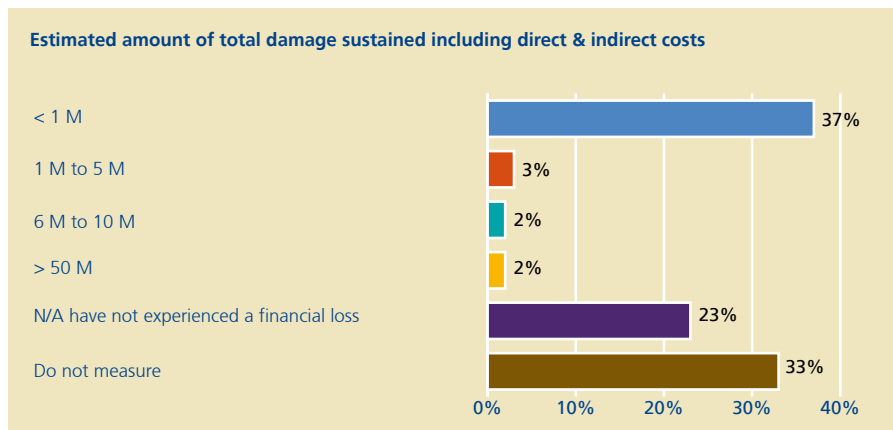


## External breaches

Advances in communication and technology have opened organizations to new forms of attack. At the same time, increased reliance on third parties has increased the complexity and likelihood of a breach from the outside. In the 12 months preceding the survey, respondents experienced a variety of external and internal breaches.

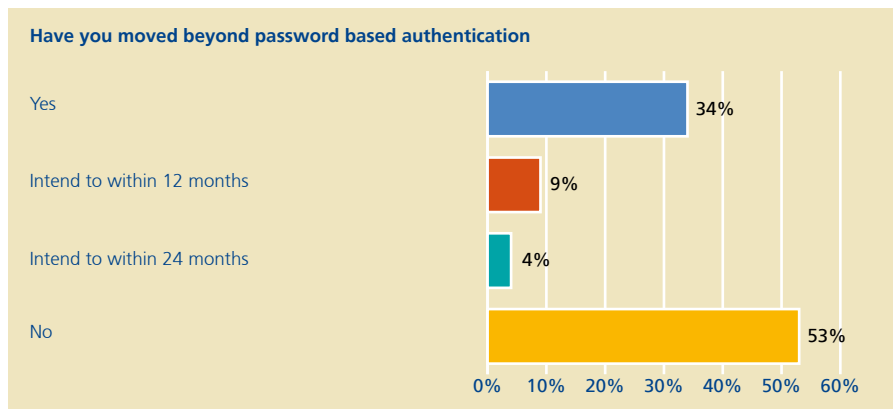


Although the greatest number of the surveyed TMT organizations (37 percent) estimated their own organization's total damage from security breaches last year to be under US\$1 million, a small number (2 percent) believe their own organization's total damage from security breaches last year exceeded US\$50 million. It should also be noted that a large number of TMT companies (33 percent) do not measure the damage from security breaches.



Damages fell into three categories: direct financial cost (40 percent), internal cost (31 percent) and reputational cost (29 percent).

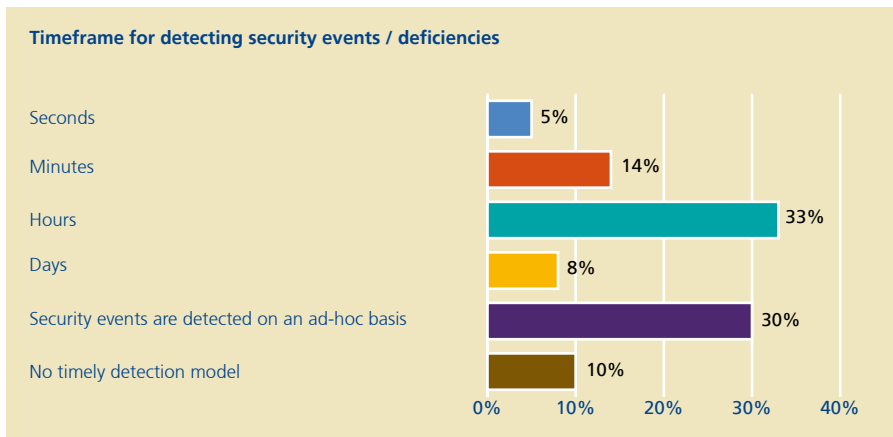
One way to reduce the number of external breaches is to move beyond password-based authentication for end user internet transactions. The survey results show that 53 percent of respondents have not done this, and these respondents do not intend to so within the next 24 months.



## Security incidents

Nearly all respondents (98 percent) investigate information security incidents upon discovery. Two-thirds (67 percent) report such incidents to law enforcement authorities when relevant, and 8 percent report all incidents. However, a surprisingly large number (25 percent) do not report any information security incidents to law enforcement authorities.

Timely detection of security events and deficiencies helps enable a company to establish countermeasures and remediate risk as soon as possible. However, this ability varies widely among the surveyed organizations.

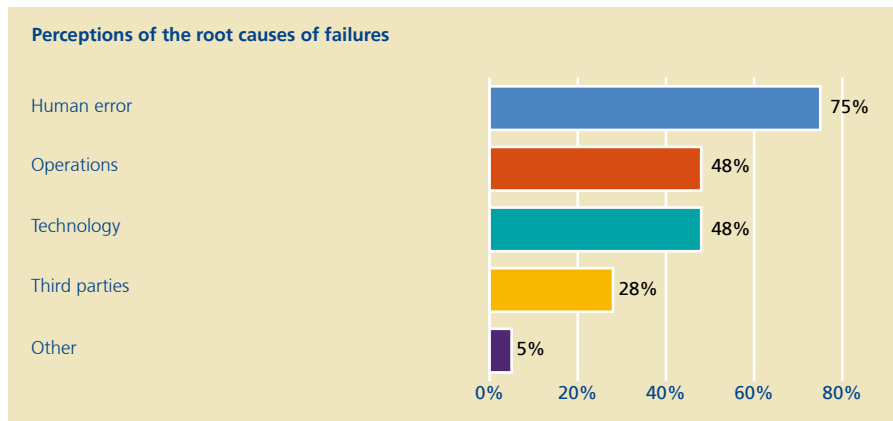


According to the survey, at most companies, detecting security events and deficiencies is primarily the responsibility of IT personnel (34 percent) or IT security personnel (41 percent). Also, the vast majority of the surveyed TMT organizations (76 percent) have implemented a management solution to manage security incidents and events.

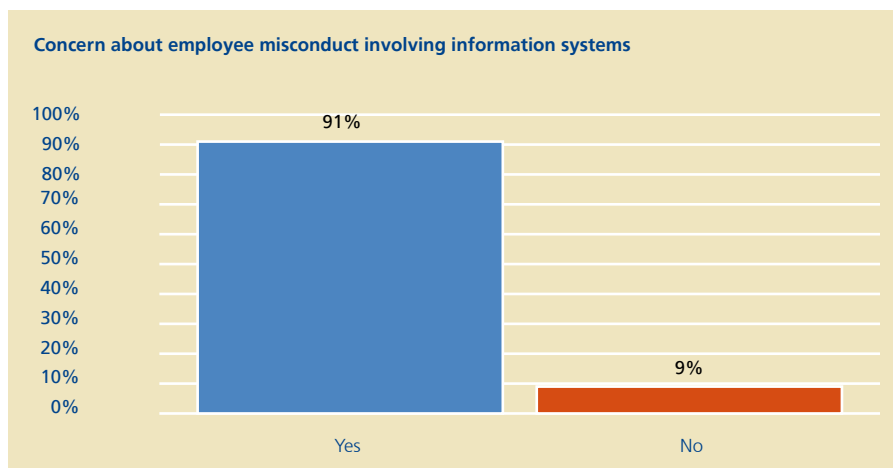
## People risk

The TMT industry is driven by an entrepreneurial spirit that places a strong emphasis on speed, flexibility, creativity, and innovation. TMT employees tend to be free spirited and tech-savvy, and TMT organizational structures generally encourage decentralized decision making, employee empowerment, informal communications, and flexible procedures. These characteristics are usually a blessing; but when it comes to information security, they can also be a curse.

According to the survey, TMT companies regard “human error” as the leading cause of security failures such as breakdowns, business interruptions, and system outages.

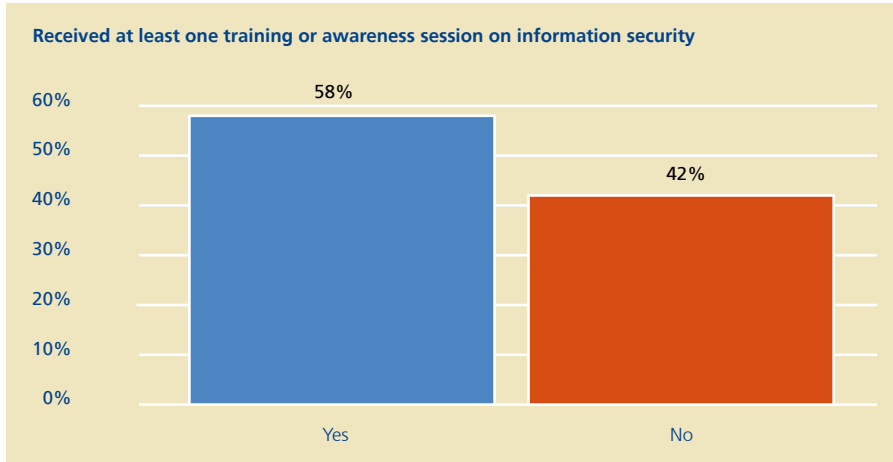


Insider threats are another people-related risk, with 91 percent of respondents indicating that employee misconduct remains a major concern for their organization. In fact, the survey data shows that mitigating the risk of employee misconduct is the number one threat-based initiative for 2007. Moreover, 47 percent of respondents say that improvements in access and identity management – which help reduce the potential for employee misconduct – will be a top operational security initiative in the coming year.

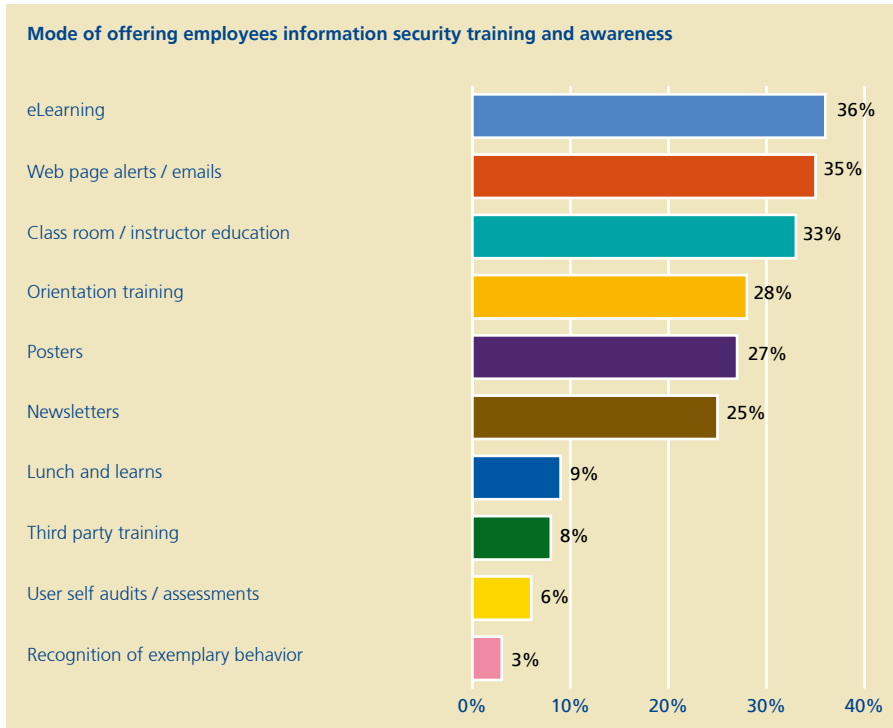


Another risk that exploits the human factor is “social engineering”. Hackers use social engineering techniques (e.g., phishing and pretexting) to trick people into disclosing confidential information. In this year’s survey, 40 percent of respondents rated social engineering as a high threat, putting it at the top of the list ahead of better-known external threats such as viruses, worms, spam, and denial of service attacks.

One of the ways to address people-related risks such as human error, employee misconduct, and social engineering is through training or awareness sessions that embed security awareness within the organization. Yet, only 58 percent of respondents provided employees with such training during the past year.



According to the survey, TMT companies deliver information security training and awareness in a variety of ways, including eLearning (36 percent), web page alerts / emails (35 percent), and traditional classroom instruction (33 percent).

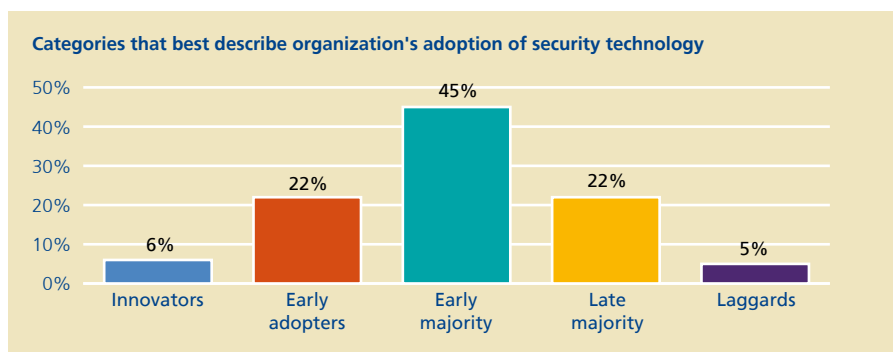


## Use of security technology

### Adopting new technology

TMT organizations face a never-ending dilemma when deciding what security technology to implement – and when. If they try to stay at the cutting edge of technology, they will probably suffer through many promising solutions that fail to meet their expectations. But if they stick with proven solutions, they are likely to find that rapid technological advances have quickly rendered their “safe bets” obsolete.

Since most TMT companies operate at the forefront of technology in their day-to-day businesses, it is not surprising to see them take a similar approach to information security. The survey shows that most TMT organizations consider themselves innovators (6 percent), early adopters (22 percent), or at least among the “early majority” (45 percent) when it comes to adopting security technology.

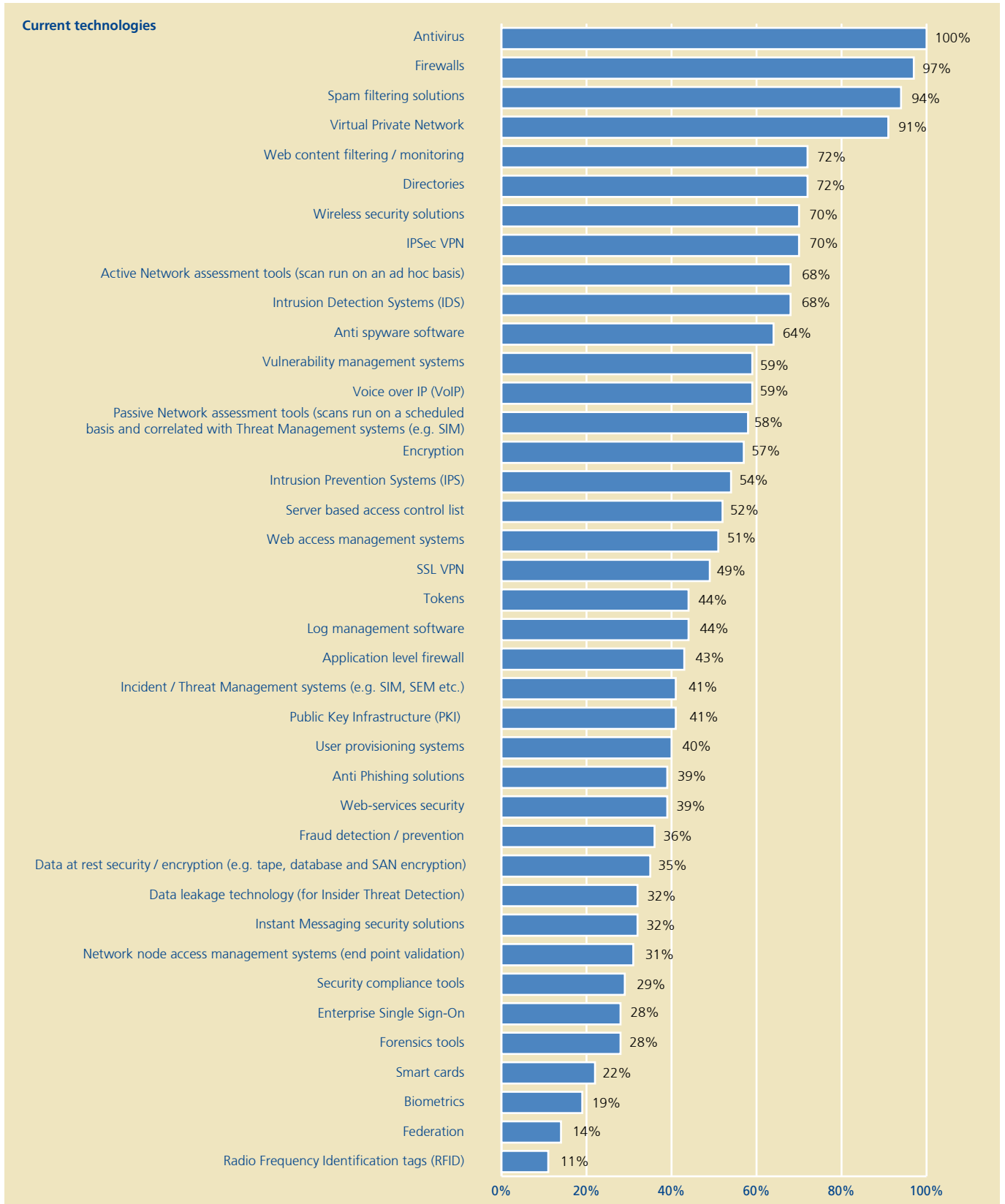


Similarly, the survey data shows that a vast majority of the TMT companies are not afraid to implement new technologies. In fact, only 25 percent say they will wait until a new technology has proven itself.

Despite the industry's general receptivity to new technology, it might make sense for even more TMT companies to take an active role in security innovation – using their technical expertise to get in front of the ever-increasing threats.

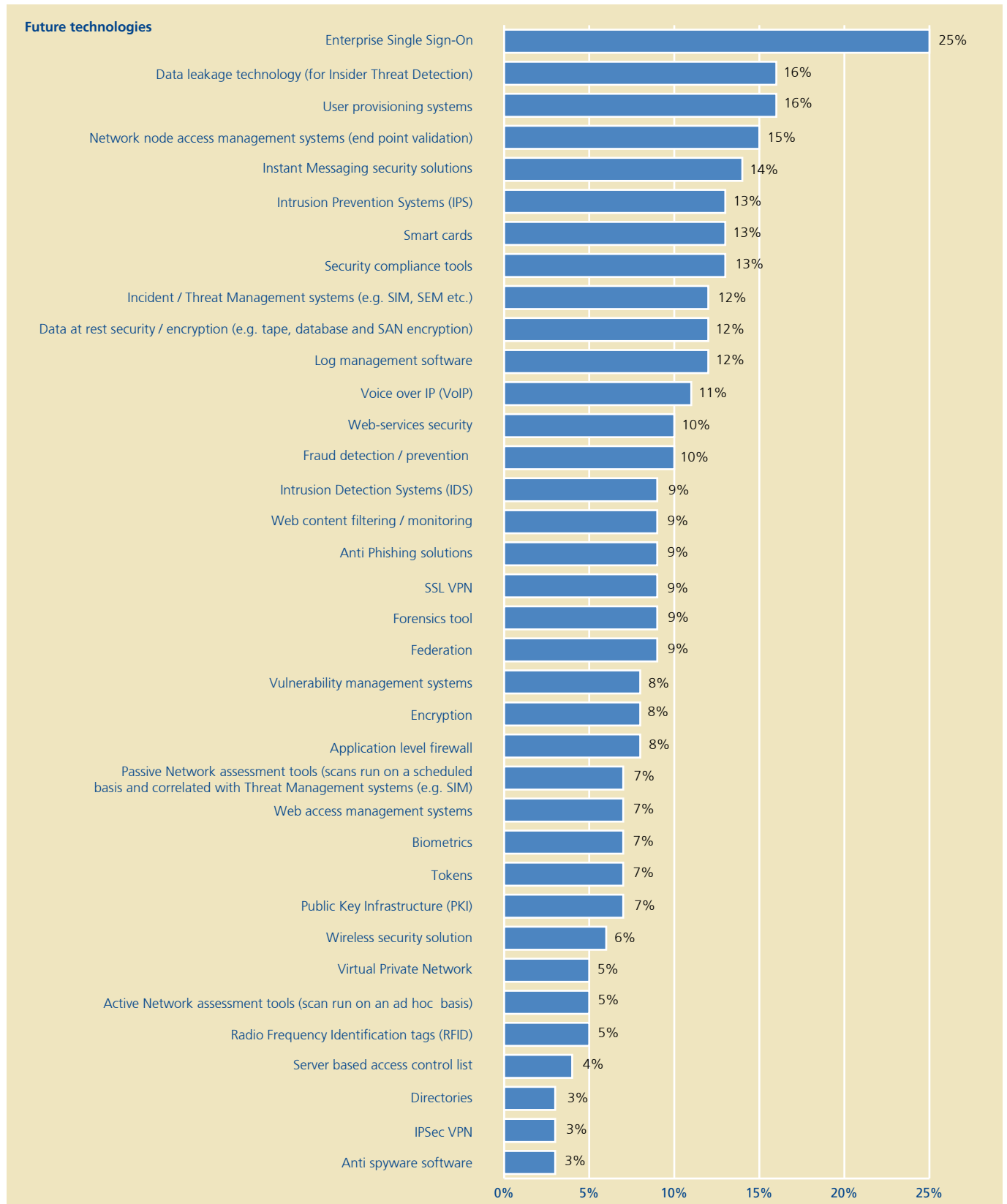
## Current technologies

The survey shows that respondents have implemented – or are currently piloting – a wide range of security technologies.

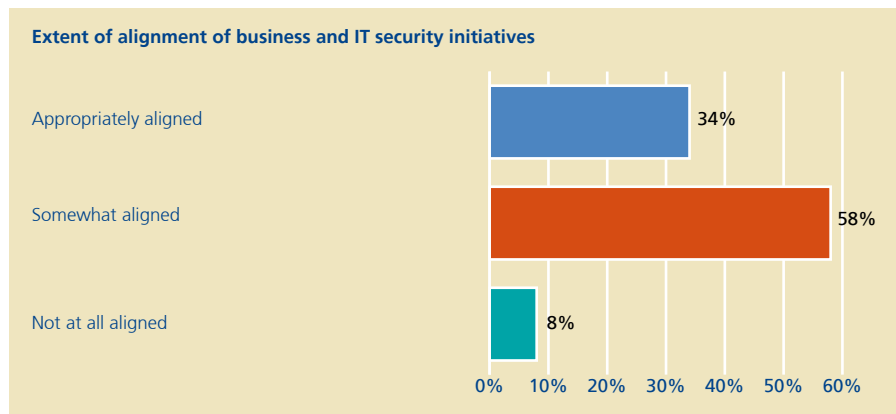


## Future technologies

Over the next 12 months, TMT companies expect to implement or pilot the following technologies:



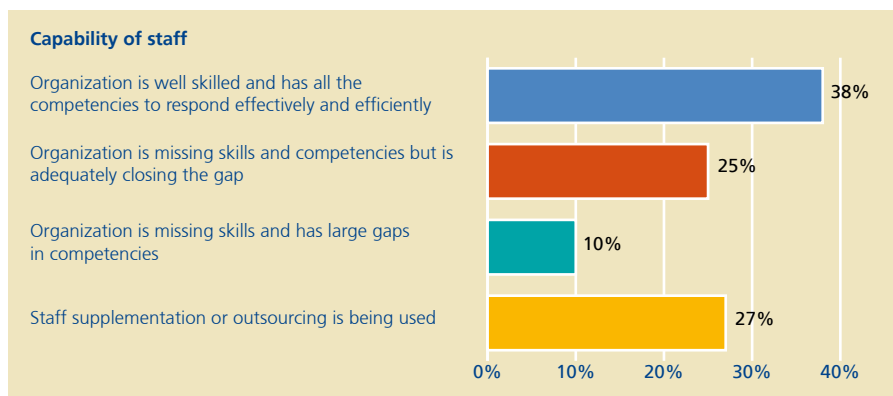
“Single Sign-On technology” tops the list of future technology initiatives. Single Sign-On improves both convenience and security, making it a good example of aligning business and IT initiatives. However, the survey shows that such alignment is often the exception, rather than the rule. In fact, 58 percent of the surveyed companies consider their business and IT security initiatives only “somewhat aligned”, while another 8 percent say they are “not at all aligned”.



## Quality of operations

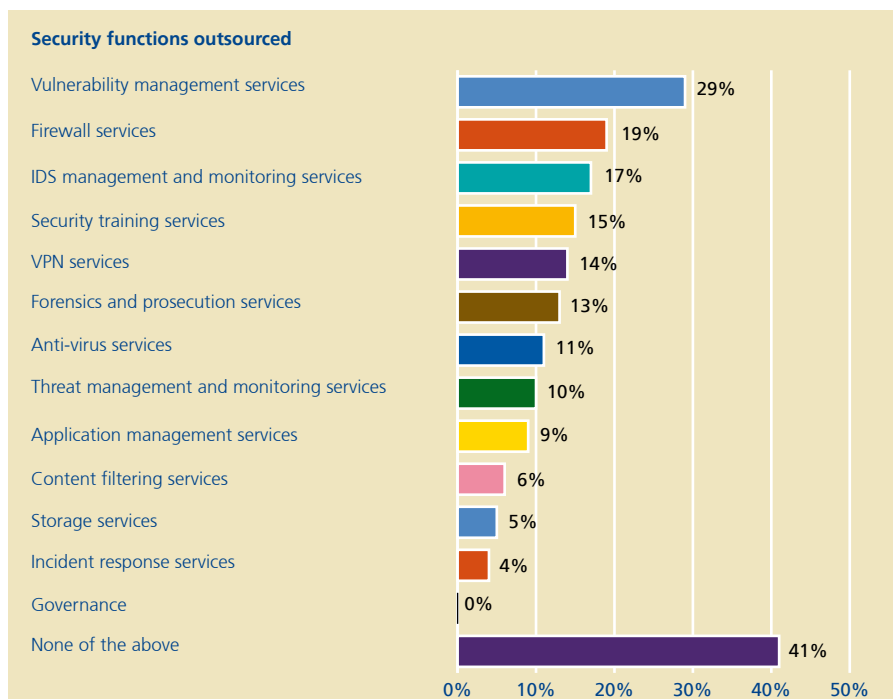
### A shortage of security skills

One of the biggest obstacles to implementing better information security, and managing information security risks, is finding staff with the appropriate skills to do the job. According to the survey, only 38 percent of TMT companies believe they have personnel with the skills and all the competencies necessary to respond effectively and efficiently to security challenges.



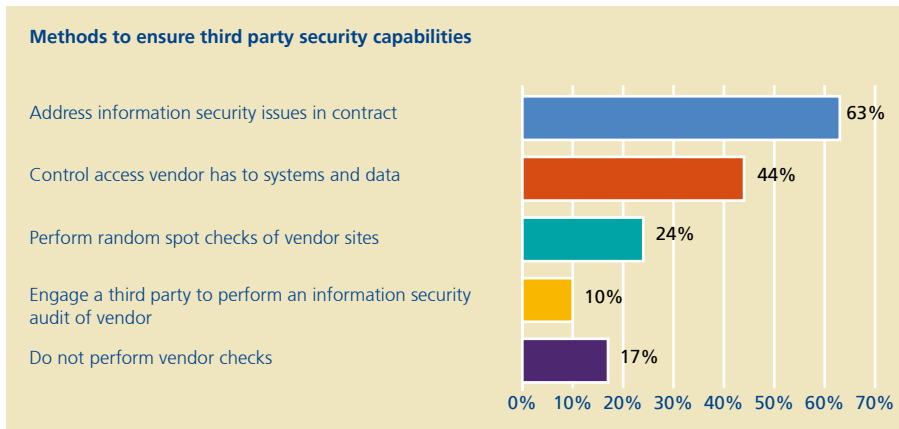
### The extended business relationship

These days, nearly all TMT companies outsource some of their business processes. However, when it comes to information security, the vast majority of activities continue to be done in house.

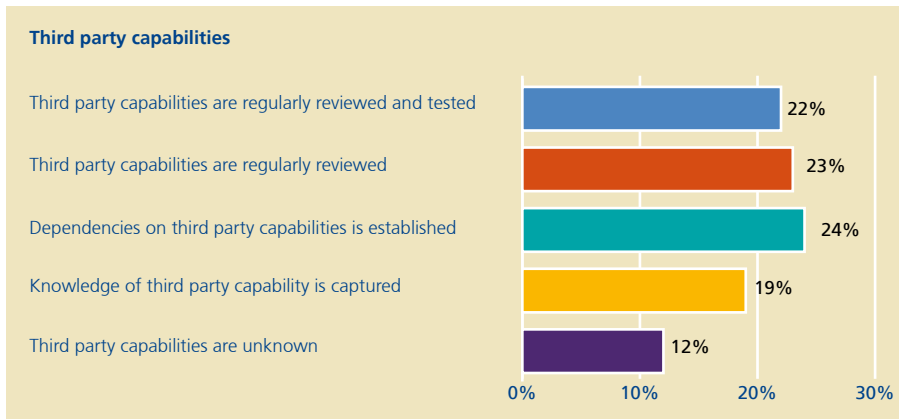


The IT security activity that is outsourced the most by respondent TMT companies is vulnerability management services – a highly specialized service that often is not readily available within a company. None of the surveyed companies outsource governance of the security function.

Given the importance and sensitivity of information security, it is essential for TMT companies to choose their outsourcing vendors wisely. Prior to signing an outsourcing contract, the surveyed TMT companies use a variety of the first four methods below to ensure that a third party’s capabilities are adequate.



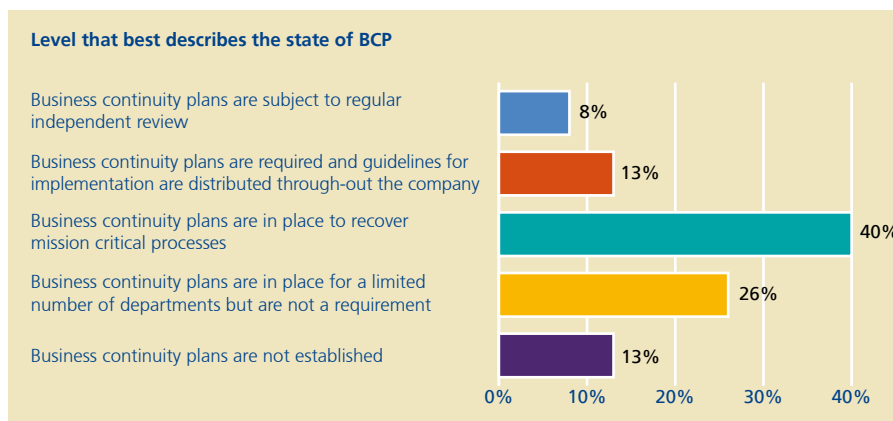
It is alarming that among the surveyed TMT companies that outsource parts of their information security, 17 percent do not perform vendor checks. Moreover, only 22 percent review and test their third parties’ capabilities on a regular basis. These deficiencies expose a company to a significant level of third-party risk.



## Staying in business

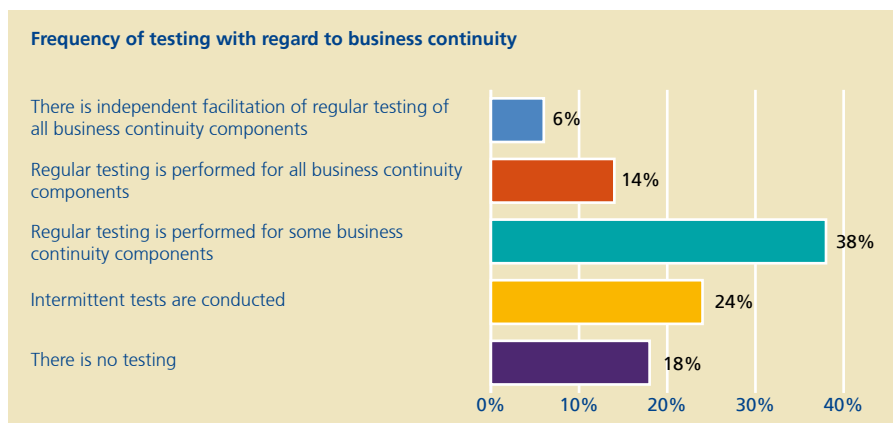
In today's competitive market, TMT companies can't afford to 'take a day off'. Customers are increasingly reliant on TMT products and services, and expect them to be available at all times. A major disruption in business operations can cause a significant hit to a company's reputation and bottom line – something the company may never recover from.

The vast majority of TMT companies recognize the importance of business continuity, and 87 percent of the respondents have established some level of business continuity plans.



According to the survey, the primary motivator for business continuity planning is to ensure operational resilience and availability. Another key motivator is to make executives and senior executives accountable for business continuity. Surprisingly, only 18 percent of the respondents say they established business continuity plans in order to protect their public image or reputation.

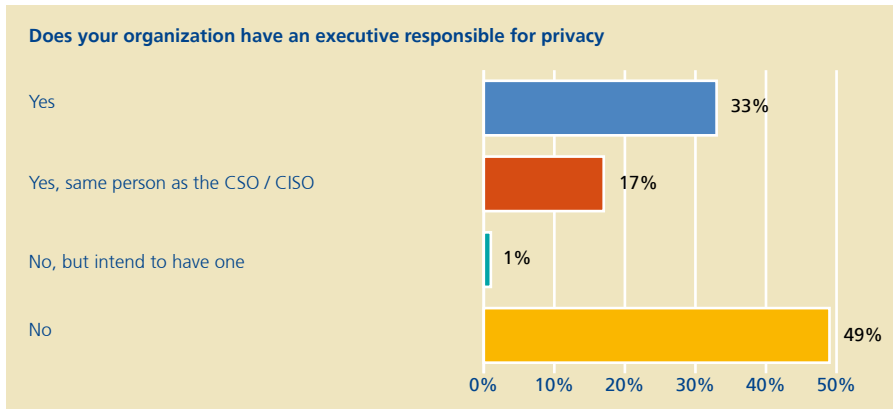
Although a business continuity plan might look good on paper, it needs to be tested on a regular basis to ensure it is reliable and effective. The survey shows that 18 percent of respondents do not test any part of their business continuity plan, which could leave them vulnerable in the event of a crisis.



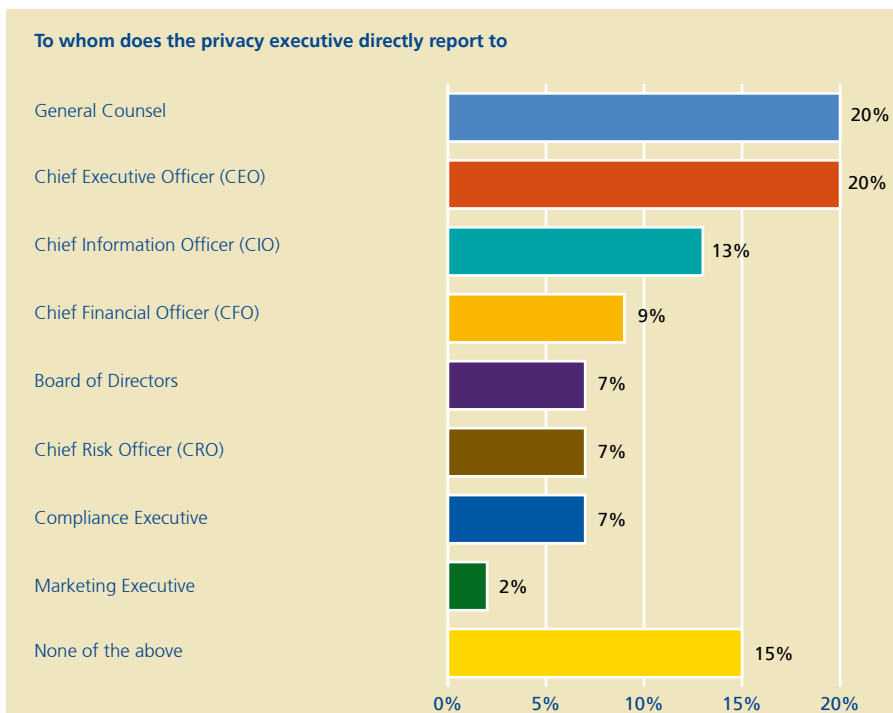
## Privacy

At first glance, privacy might not seem like big deal for TMT companies. However, organizations that have any contact with personal information – even during a brief transaction – increasingly find themselves facing a whole host of privacy-related issues driven by a combination of legislation, industry self-regulation, legal liability, and customer expectations.

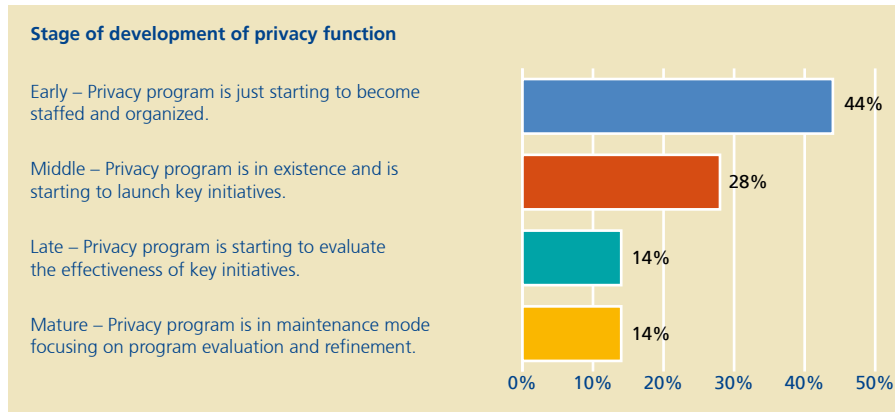
This year’s survey shows that 50 percent of TMT companies have an executive who is responsible for privacy within the organization. For 17 percent, this executive is the Chief Security Officer or Chief Information Security Officer.



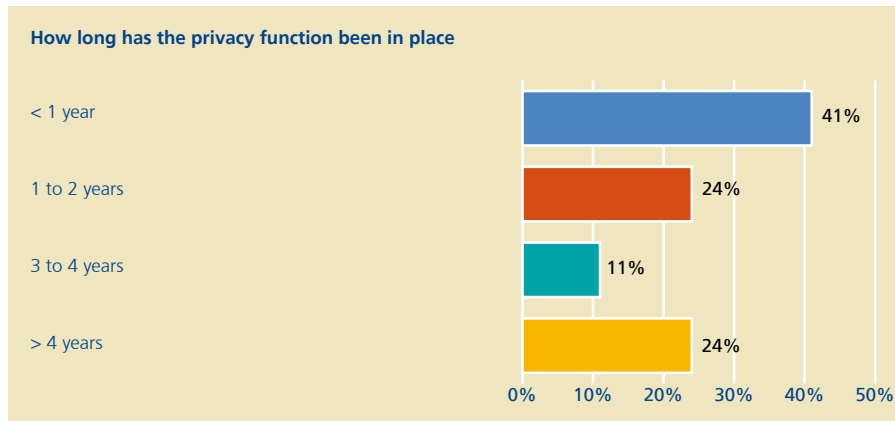
According to the survey, a small percentage of privacy executives report directly to the CEO (20 percent) or board of directors (7 percent). This suggests that many of the surveyed TMT companies do not view privacy as a strategic business issue.



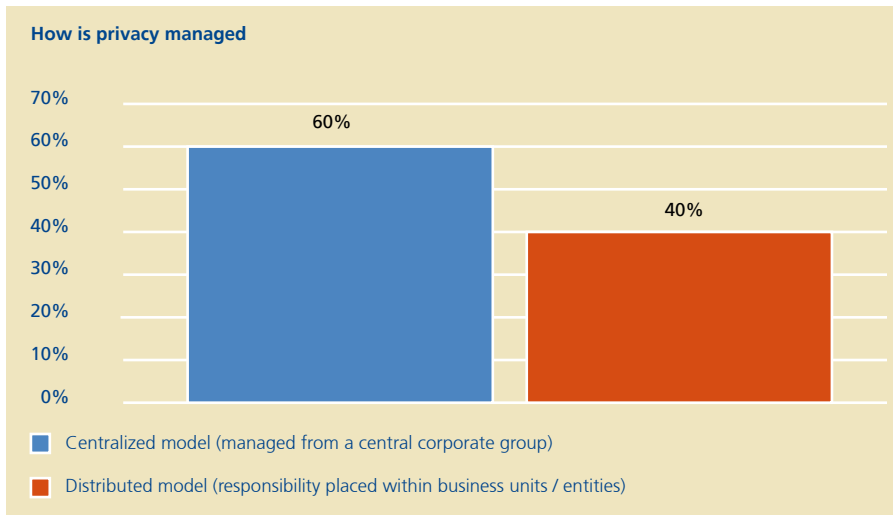
Yet the privacy issue seems to be growing in importance. According to the survey, many TMT companies (44 percent) acknowledge that their privacy program is just starting to get staffed and organized. Another 28 percent have a privacy program in place but are still in the process of launching key initiatives.



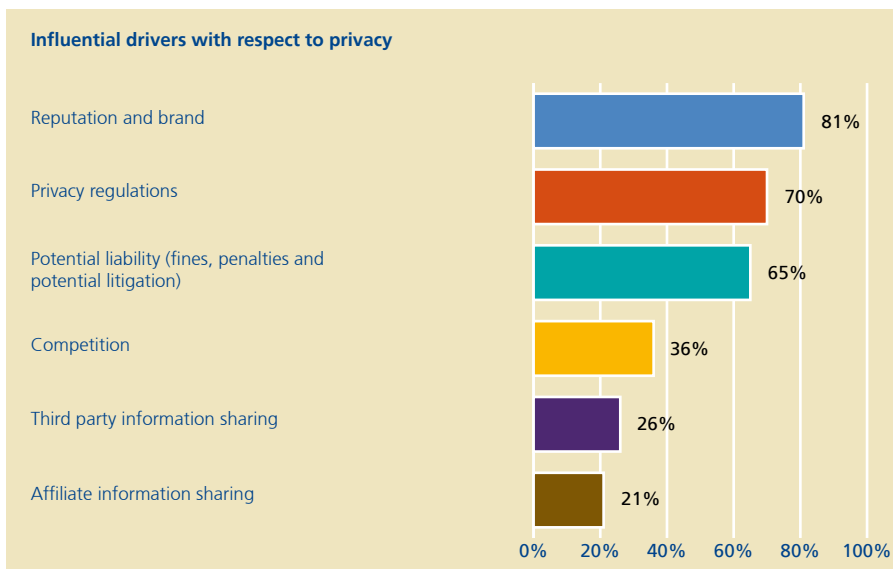
Among the surveyed companies, 41 percent say their privacy function has only been in place for less than a year, and only 24 percent have had the function in place longer than 4 years.



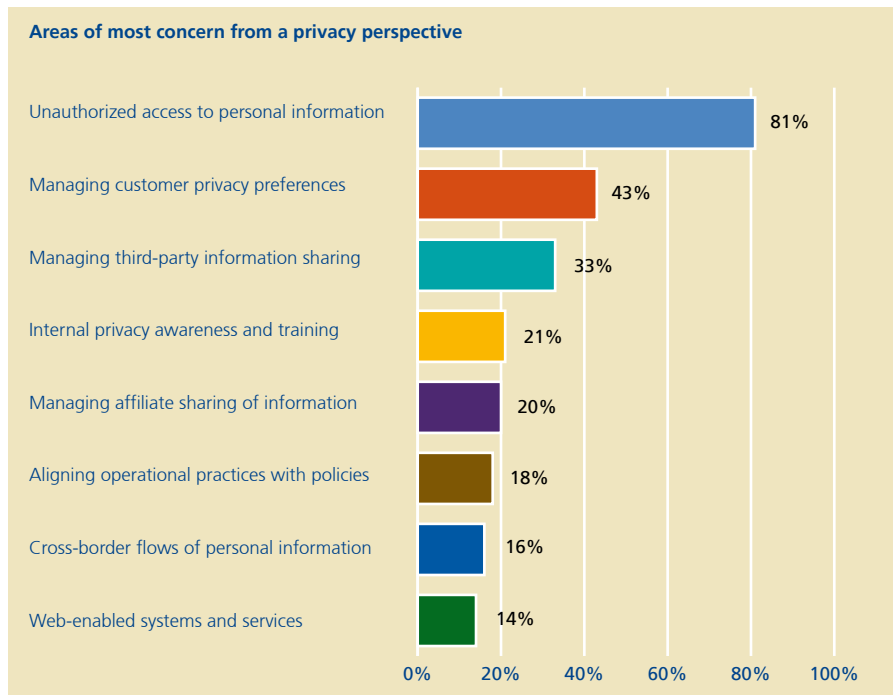
The best approach for managing privacy issues seems open to debate. In this year’s survey, 60 percent of respondents use a centralized model where privacy issues are managed from a central corporate group, while the other 40 percent use a distributed model where primary responsibility lies with the business units.



To be effective, privacy programs and initiatives should be designed around a wide range of factors, including reputation and brand, privacy regulations, potential liability, and competitive strategy.



Privacy is a complex challenge spanning a wide range of areas. However, according to the survey, the biggest concern is preventing unauthorized access to personal information.



Among the TMT companies surveyed, 19 percent are in the process of creating an inventory of the personal information within their organization. However, almost half (49 percent) have not performed such an inventory. It is difficult for an organization to protect its customers' personal information if it does not know what it has, or where the personal information is located.

Loss of customer data can be disastrous for both a company and its customers. In many cases, the law requires a company to disclose such losses. However, even when disclosure is not legally mandated, organizations should track these incidents in order to manage the damage and address their root causes. Yet, according to the survey results, 36 percent of TMT companies do not track or publicly report any loss of customer data. Another 29 percent do not report such losses unless required to do so.

# Digital Rights Management (DRM)

## A digital dilemma

Almost all companies within the TMT industry have a business model that revolves around digital assets and intellectual property. These companies face an overwhelming challenge; how to protect an asset that can be effortlessly duplicated and distributed? Current copyright laws struggle to meet the needs of a rapidly changing market based on digital content, where each use produces a perfect copy of the original.

TMT organizations face the dilemma of making their precious assets available without protection, or finding and implementing ways to protect and restrict the use of those assets. The systems and tools for protecting digital assets from unauthorized duplication are known as Digital Rights Management (DRM).

The current market appears to be divided on the topic of DRM, and there is no clear-cut answer to suit all organizations. One option that seems to be gaining ground is to do away with DRM altogether. The reasoning is that DRM creates an inconvenience for customers (making them less likely to buy the product), is complicated and costly for a company to implement and maintain, and is bound to be circumvented at some point anyway.

## IP protection

In addition to protecting their digital content, TMT organizations are rightfully concerned about protecting their intellectual property (IP). Whether their IP is of strategic importance (such as the development of a new product), or operational importance, the theft or loss of critical IP can have disastrous consequences.

The survey shows that IP protection is a high priority for many organizations, with 66 percent of respondents identifying IP loss or theft as a specific security risk. At the same time, however, 23 percent of respondents say that no specific security measures have been implemented.



## The Future of DRM

Each sector in the TMT industry faces different risks. Therefore, a universal approach to DRM seems unlikely. Among the surveyed companies, 61 percent expect the use of DRM to increase over the next three years. However, most expect DRM to be expensive and / or difficult to implement. TMT organizations should carefully assess their own situation and choose the course of action that aligns with their unique requirements.

# Design, implementation & evaluation of the survey

The 2007 DTT TMT Global Security Survey reports on the outcome of focused discussions between DTT TMT Industry Group's professionals and the information technology executives of global TMT companies.

Discussions with the information technology executives of these organizations were designed to identify, record, and present the state of the practice of information security in the TMT industry with a particular emphasis on identifying levels of perceived risks, the types of risks with which TMT companies are concerned and the resources being used to mitigate these risks. The survey also identifies which technologies are being implemented to improve security and the value TMT companies are gaining from their security and privacy investments. To fulfill this objective, senior professionals of the DTT Security & Privacy Services Group designed a questionnaire that probed seven aspects of strategic and operational areas of security and privacy. These seven areas are described in the section entitled 'Areas covered by the survey'.

Responses of participants relating to the seven areas of the questionnaire were subsequently analyzed and consolidated and are presented herein in both qualitative and quantitative formats.

## Drafting of the questionnaire

The questionnaire was comprised of questions composed by the survey team made up of senior DTT Security & Privacy Services Group professionals. Questions were selected based on their potential to reflect the most important operating dimensions of a TMT company's process or systems in relation to security and privacy. The questions were each tested against global suitability, timeliness, and degree of value. The purpose of the questions was to identify, record, and present the state of information security and privacy in the TMT industry. New questions were also added to reflect topics being asked about by DTT member firms' clients and raised by the media.

## 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 related to the identified areas. Each participating region assigned responsibility to senior professionals of the DTT member firms' Security & Privacy Services practices and those people were held accountable for obtaining answers from the various TMT companies with which they had a relationship. 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. The DTT TMT Industry Group also offered pre-selected TMT companies the ability to submit answers online using an online questionnaire managed by DeloitteDEX. Data was collected from May through December 2007.

## Results analysis and validation

DeloitteDEX and Deloitte Research-Survey Advisory Services were responsible for analyzing and validating the data from the survey. DeloitteDEX is a family of proprietary products and processes for diagnostic benchmarking applications. DeloitteDEX uses a variety of research tools and information databases to provide benchmarking analyses measuring financial and / or operational performance. Clients' performance can be measured against that of their peer group(s). The process identifies competitive performance gaps and allows management to understand how to improve the performance of business processes by identifying and adopting leading practices on a company, industry, national or global basis, as appropriate.

Deloitte Research-Survey Advisory Services used a variety of research and statistical tools to provide extensive analysis and interpretation of the survey results. Some answers to specific questions were not used in calculations to keep the analysis simple and straightforward. If respondents did not answer a question, the count for that question was adjusted accordingly. For some questions, respondents were able to select multiple answers, in which case the survey percentages exceed 100%.

## Acknowledgements

We wish to thank all of the professionals of the TMT companies who responded to the survey and who allowed us to further correspond with them over the course of this project. Without such participation and commitment, the DTT TMT Industry Group could not produce surveys such as this. We extend our thanks for the time and effort that respondents devoted to this project.

# Contacts

**Igal Brightman**

Global Managing Partner  
Deloitte Touche Tohmatsu  
Technology, Media &  
Telecommunications  
+972 3 608 55 00  
ibrightman@deloitte.co.il

**Mark Layton**

Global Enterprise Risk Services Leader  
Deloitte & Touche LLP  
United States  
+1 214 840 7979  
mlayton@deloitte.com

Regional leaders

**Adel Melek**

Canada – Toronto  
Deloitte & Touche LLP  
+1 416 601 6524  
amelek@deloitte.ca

**Christopher Lee**

USA – San Jose  
Deloitte & Touche LLP  
+1 408 704 4314  
chrislee@deloitte.com

**Simon Owen**

EMEA – London, UK  
Deloitte & Touche LLP UK  
+44 20 7303 7219  
sxowen@deloitte.co.uk

**Uantchern Loh**

APAC – Kuala Lumpur, Malaysia  
Deloitte KassimChan  
+65 6216 3282  
uloh@deloitte.com

**Bruce Daly**

Japan – Tokyo, Japan  
Deloitte Touche Tohmatsu  
+81 3 4218 7284  
brdaly@deloitte.com

**Mitsuhiko Maruyama**

Japan – Tokyo, Japan  
Deloitte Touche Tohmatsu  
+81 3 3457 7321  
mitsuhiko.maruyama@deloitte.com

Americas

**Alberto Lopez Carnabucci**

Argentina  
+54 11 4320 2700  
alopezcarnabucci@deloitte.com

**Marco Antonio Brandao Simurro**

Brazil  
+55 11 5186 1232  
mbrandao@deloitte.com.br

**John Ruffolo**

Canada  
+1 416 601 6684  
jruffolo@deloitte.ca

**Arturo Platt**

Chile  
+56 2 2703 361  
aplatt@deloitte.com

**Elsa Victoria Mena Cardona**

Colombia  
+571 546 1815  
emenacardona@deloitte.com

**Carlos Gallegos Echeverria**

Costa Rica  
+506 253 2466  
cagallegos@deloitte.com

**Ernesto Graber**

Ecuador  
+593 4 245 2770 ext 1663  
egraber@deloitte.com

**Francisco Silva**

Mexico  
+52 55 5080 6310  
fsilva@dtm.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  
+1 203 708 4860  
pasmundson@deloitte.com

**Robert de Luca**

Uruguay  
+598 2 916 0756 ext 123  
rdeluca@deloitte.com

**Hector Gutierrez**

Venezuela  
+58 212 206 8534  
hgutierrez@deloitte.com

Europe/Middle East/Africa

**Georg Kraus**

Austria  
+43 1 537 00 4810  
gkraus@deloitte.at

**Carlo Schupp**

Belgium  
+32 2 800 20 77  
cschupp@deloitte.com

**Dariusz Nachyla**

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

**Gennady Kamyshnikov**

Commonwealth of  
Independent States  
+7 495 787 0600  
gkamyshnikov@deloitte.ru

**Kim Gerner**

Denmark  
+45 36 10 32 81  
kgerner@deloitte.dk

**Jussi Sairanen**

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

**Francois Renault**

France  
+33 1 55 61 61 22  
frenault@deloitte.fr

**Andreas Gentner**

Germany  
+49 711 1655 47302  
agentner@deloitte.de

Europe/Middle East/Africa

**Dieter Schlereth**

Germany  
+49 211 8772 2638  
dschlereth@deloitte.de

**Tom Cassin**

Ireland  
+353 1 417 2210  
tcassin@deloitte.ie

**Asher Mechlovich**

Israel  
+972 3 608 5524  
amechlovich@deloitte.co.il

**Alberto Donato**

Italy  
+39 064 780 5595  
adonato@deloitte.it

**Dan Arendt**

Luxembourg  
+352 451 452621  
darendt@deloitte.lu

**Saba Sindaha**

Middle East  
+971 2 646 0606  
ssindaha@deloitte.com

**Jacques Buith**

Netherlands  
+31 20 454 7066  
jbuith@deloitte.nl

**Halvor Moen**

Norway  
+47 2327 9785  
hmoen@deloitte.no

**Joao Luis Silva**

Portugal  
+351 210 427 635  
joaosilva@deloitte.pt

**Kris Budnik**

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

**Eduardo Sanz**

Spain  
+34 91 514 5000  
edsanz@deloitte.es

**Tommy Maartensson**

Sweden  
+46 8 506 711 30  
tommy.maartensson@deloitte.se

**Baris Oney**

Turkey  
+90 212 366 6073  
boney@deloitte.com

**James Alexander**

United Kingdom  
+44 20 7007 3264  
jalexander@deloitte.co.uk

Asia Pacific

**Damien Tampling**

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

**Charles Yen**

Hong Kong / China  
+86 10 8520 7000  
chyen@deloitte.com.cn

**N. Venkatram**

India  
+91 22 5667 9125  
nvenkatram@deloitte.com

**Yoshitaka Asaeda**

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

**Hyun Chul Jun**

Korea  
+82 2 6676 1307  
hjun@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  
clarkchen@deloitte.com.tw

**Marasari Kanjanataweewat**

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

TMT marketing contacts

**Noel Spiegel**

United States  
Deloitte & Touche LLP  
Partner in charge of DTT TMT  
Marketing  
+1 212 492 4135  
nspiegel@deloitte.com

**Francois Van Der Merwe**

Australia  
Director of DTT TMT Marketing  
+612 9322 5406  
francoisvandermerwe@deloitte.com.au

**Amanda Goldstein**

United States  
DTT TMT Marketing  
+1 212 436 5203  
agoldstein@deloitte.com

**Yvonne Dow**

Hong Kong / China  
Director of Asia Pacific TMT  
Marketing  
+852 2852 6611  
ydow@deloitte.com

# About TMT

The Deloitte Touche Tohmatsu (DTT) Technology, Media & Telecommunications (TMT) Industry Group consists of the TMT practices organized in the various member firms of DTT and includes more than 6,000 member firms' partners, directors and senior managers supported by thousands of other professionals dedicated to helping their clients evaluate complex issues, develop fresh approaches to problems and implement practical solutions.

There are dedicated TMT member firms' practices in 45 countries and centers of excellence in the Americas, EMEA and Asia Pacific. DTT member firms serve nearly 90 percent of the TMT companies in the Fortune Global 500. Clients of DTT member firms' TMT practices include some of the world's top software companies, computer manufacturers, wireless operators, satellite broadcasters, advertising agencies and semiconductor foundries – as well as leaders in publishing, telecommunications and peripheral equipment manufacturing.

# About the DTT ERS Security & Privacy Group

The ongoing mission of the Security & Privacy Services team is to work with clients to achieve robust security through the delivery of end-to-end solutions, by world-class experienced professionals, utilizing proven methodologies and tools, in a consistent manner globally. By working together, Deloitte member firms can assist you in improving enterprise security and value, bring new solutions to market and develop risk aware programs and processes.

The Security & Privacy services are part of Enterprise Risk Services (ERS). Deloitte member firms have over 10,000 people helping clients manage risk and uncertainty, from the boardroom to the network. Deloitte member firms provide a broad array of services that allow clients around the world to better measure, manage and control risks to enhance the reliability of systems and processes.

DTT member firms' enterprise-wide services include:

- Application security / integrity
- Business Continuity Management
- Identity and Access Management
- Infrastructure and operations security
- Privacy and data protection
- Security management
- Vulnerability management

Member firms' resources include over 900 Certified Information Systems Security Professionals (CISSP) across DTT member firms, presence in more than 80 cities, access to 26 global technology centers, and access to technology solution sets developed through long standing vendor alliances.



For more information on the 2007 DTT TMT Global Security Survey, please contact the TMT marketing contacts or DTT member firm professional listed in the 'Contact' section of this publication.

**Disclaimer**

These materials and the information contained herein are provided by Deloitte Touche Tohmatsu and are intended to provide general information on a particular subject or subjects and are not an exhaustive treatment of such subject(s). Accordingly, the information in these materials is not intended to constitute accounting, tax, legal, investment, consulting or other professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

Survey users should be aware that Deloitte Touche Tohmatsu has made no attempt to verify the reliability of such information. Additionally, the survey results are limited in nature, and do not comprehend all matters relating to security and privacy that might be pertinent to your organization.

These materials and the information contained herein are provided as is, and Deloitte Touche Tohmatsu makes no express or implied representations or warranties regarding these materials or the information contained herein. Without limiting the foregoing, Deloitte Touche Tohmatsu does not warrant that the materials or information contained herein will be error-free or will meet any particular criteria of performance or quality. Deloitte Touche Tohmatsu expressly disclaims all implied warranties, including, without limitation, warranties of merchantability, title, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy.

Prediction of future events is inherently subject to both known and unknown risks, uncertainties and other factors that may cause actual results to vary materially. Your use of these materials and the information contained herein is at your own risk and you assume full responsibility and risk of loss resulting from the use thereof. Deloitte Touche Tohmatsu will not be liable for any special, indirect, incidental, consequential, or punitive damages or any other damages whatsoever, whether in an action of contract, statute, tort (including, without limitation, negligence), or otherwise, relating to the use of these materials or the information contained herein.

If any of the foregoing is not fully enforceable for any reason, the remainder shall nonetheless continue to apply.

**About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in over 140 countries. With access to the deep intellectual capital of approximately 150,000 people worldwide, Deloitte delivers services in four professional areas – audit, tax, consulting, and financial advisory services – and serves more than 80 percent of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms have any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names.

©2007 Deloitte Touche Tohmatsu. All rights reserved.

