PROBLEM
DRIVEN
RESEARCH

advanced series

Foundation

CONSUMER GOODS & RETAIL 2

2013 No. 02

Security Solutions
in Consumer Goods & Retail

IE FOUNDATION ADVANCED SERIES ON PROBLEM-DRIVEN RESEARCH

ERNST & YOUNG
Quality In Everything We Do

ie foundation

Greetings

Dear friends:

One of IE Business School's goals is to be an international center of excellence for research in all areas of management. We pursue this goal in close collaboration with the IE Foundation and the recently established IE University.

I would like to present a new initiative of the IE Foundation and IE Business School. We hope it will provide an innovative way to share the results of the joint work of our scholars and partner organizations.

The initiative, "IE Foundation Advanced Series on Problem Driven Research", aims to provide support to organizations facing the new economic structure, featuring unique market rules. Recognizing the importance of retailing for assessing the current situation and the social expectations, we have chosen the "Consumer Goods & Retail" series as our maiden work.

The IE Business School seeks to create an environment where we can develop the best talent, while at the IE Foundation we seek to close the loop between the school and businesses by fostering sustainable relationships through the organization.

We are confident that this initiative will meet the challenge and offer a new perspective on the issues.

Marco Trombetta
Vice-dean of Research at IE Business School
Vice-dean Coordination and Research IE University

ie foundation

contents

Lead researcher

IE Foundation cover letter

Ernst & Young cover letter

Executive summary

01 Technology trends in the Consumer Goods & Retail sector

02 Cloud computing in the Consumer Goods & Retail sector
2.1 Challenges of cloud computing adoption
2.2 Recommendations for cloud technology usage
2.3 Case study: Reliability in the event of a cloud services provider failure

03 Social media in the Consumer Goods & Retail sector
3.1 Understanding the risks of social media
3.2 Brand protection in social media
3.3 Case study: Hacking of a CEO's twitter account

04 Connecting in a mobile world
4.1 Mobile device risks
4.2 Mobile device security recommendations
4.3 Case study: When a free app becomes expensive

05 Data loss
5.1 Challenges of data loss management
5.2 Recommendations for managing data loss
5.3 Case study: TJX data breach

06 Ernst & Young viewpoint

Lead researcher

Álvaro Arenas Sarmiento

Professor of Information Systems and Head of the Information Systems and Technologies Department of IE Business School..

Álvaro Arenas is Professor of Information Systems and Head of the Information Systems and Technologies Department at the IE Business School. He holds a M.Sc. and a D.Phil. in Computation from Oxford University, and a M.Sc. in Systems Engineering and Computation from Universidad de los Andes, Colombia.

Alvaro's main research interest lies in trust and security in distributed information systems. His research has been published in a number of top tier economic journals, including IEEE Computer, Security and Communication Networks Journal, Internet Computing and Springer Journal of Grid Computing.

He is currently a member of the Scientific Advisory Board of the EU Contrail project and leads the topic of "trust and security in large-scale distributed systems" within the ERCIM CoreGRID Working Group. He was the scientific coordinator of the EU GridTrust project and led the security work in the EU XtreemOS project. He has been a keynote speaker on security in Clouds and Grids at conferences such as CloudComp 2010, CCC 2009 and CLEI 2005.

Rafael Puyol
Vice-President,
IE Foundation

Margarita Velásquez
General Director,
IE Foundation

ie foundation

Among its primary activities, IE Foundation supports the research and the knowledge sharing endeavors of IE Business School's professors. Through its initiatives IE Foundation contributes to the positioning of IE Bvusiness School as a center of excellence for innovation, and for the creation of knowledge targeted at its productive environment.

The IE Foundation aims to create strong ties and alliances with prestigious, public and private, institutions, particularly those in the business domain that can help propel our researchers' initiatives. As an institution that pursues excellence, research activities are driven by academic rigor and the utilitarian nature seeking to create knowledge. We aim to push innovation and competitiveness to provide answers to the challenges and needs of society.

This publication is part of the IE Foundation's collection on Consumer Goods and Retail, developed in collaboration with Ernst & Young. We would like to extend our gratitude to them for their commitment and their vast experience on this matter.

The collection has been designed with the purpose of analyzing the key aspects of the industry through a practice-driven, up to date perspective on key aspects of the industry such as Sustainability, Information Security, Pricing, and Profit Protection. We are in the midst of a major change in the retail industry. The challenge many Spanish organizations face, is being at the forefront of such change and benchmarking best practices in the global market. The IE Foundation looks forward to helping organizations in this process.

We hope that this publication will be of interest to you, and we appreciate your support.

José Luis Ruíz Expósito
Partner and Head of Consumer Goods & Retail

Manuel Fernández
Business Development Director Consumer Goods & Retail

ERNST & YOUNG
Quality In Everything We Do

Consumer Products and Retail companies are developing their business in a much more complex and volatile environment than they have in the past. In this environment, companies' actions focus on transforming their business processes and protecting their operational margins.

In its commitment to innovation and value creation, Ernst & Young has propelled research projects on the issues that will help companies deal with today's industry challenges.

Our research takes into account different actions regarding price dynamics from a brand differentiation perspective. Secondly, we take on the negative economic effect of shrinkage with an analytical approach, to identify its root causes and suggest corrective actions for its mitigation (profit protection). We also seek ways to preserve the information security of an industry that operates, with an increasing frequency, in mobile scenarios and technologies. Finally, we propose the adoption of a business commitment perspective, betting on sustainable initiatives from retailers that take into account manufacturers and consumers. These four areas are experiencing a large change in process. Ernst & Young and the IE Foundation are approaching these challenges from an innovative perspective with the intention of putting them into practice and creating value for the business environment.

Executive summary

Technology is evolving constantly and so is the way we use technology in our daily lives. To a greater or lesser extent, cloud computing, social media, and mobile devices are part of our lives. What new risks do companies face when implementing new technologies for use by employees and customers?

This study looks at these technologies in the Consumer Goods & Retail industry. It discusses the new risks facing companies as a result of the changes brought on by the tech revolution and recommends ways to mitigate them.

Industry players must embrace new technologies if they want to remain competitive. However, this type of change to business models increases exposure to risk and, therefore, cannot be made without exerting control. As a result, measures must be adopted to avoid the new problems facing companies.

In cloud computing, for instance, the main risks entail data integrity and privacy, regulatory compliance and management of cloud service providers.

Our recommendations include having clear security and supplier governance policies, drafting continuity plans, and following security and industry standards.

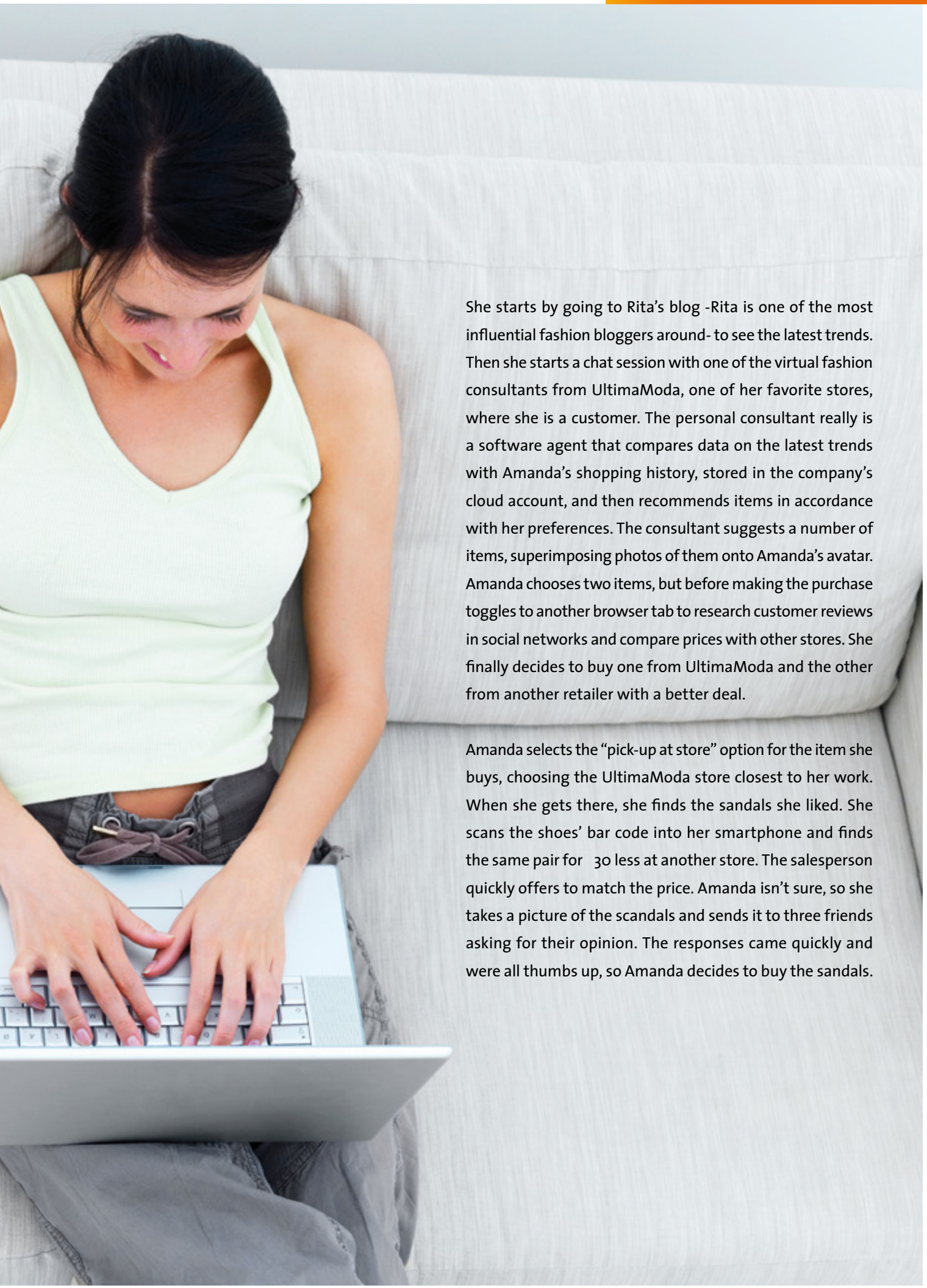
Social networks present security and reputational risks, among others. We recommend drawing up a protection strategy in social media with firm support of senior management, designing policies and user guidelines, and developing social media monitoring strategies and a procedure for addressing issues.

Risks related to the use of mobile devices include theft or loss of the devices, user administration of the devices and the existence of malware through applications (apps). Recommendations include designing clear policies governing the use of mobile devices, taking security measures with devices, and raising awareness among employees.

All these technologies are exposed to data leakage. We recommend companies pinpoint and classify business-sensitive data, assess risks in all existing communication channels, define precisely the flow of data to third parties, and set up a program from handling incidents.

1. Technology trends in *Consumer Goods & Retail*

It's a chilly Saturday afternoon in November, but Amanda, age 30 from Madrid, needs summer clothes for her upcoming Caribbean vacation. Years ago, Amanda would have gone straight to the closest mall. Today, she starts shopping on Internet from the comfort of her couch at home.



She starts by going to Rita's blog -Rita is one of the most influential fashion bloggers around- to see the latest trends. Then she starts a chat session with one of the virtual fashion consultants from UltimaModa, one of her favorite stores, where she is a customer. The personal consultant really is a software agent that compares data on the latest trends with Amanda's shopping history, stored in the company's cloud account, and then recommends items in accordance with her preferences. The consultant suggests a number of items, superimposing photos of them onto Amanda's avatar. Amanda chooses two items, but before making the purchase toggles to another browser tab to research customer reviews in social networks and compare prices with other stores. She finally decides to buy one from UltimaModa and the other from another retailer with a better deal.

Amanda selects the "pick-up at store" option for the item she buys, choosing the UltimaModa store closest to her work. When she gets there, she finds the sandals she liked. She scans the shoes' bar code into her smartphone and finds the same pair for 30 less at another store. The salesperson quickly offers to match the price. Amanda isn't sure, so she takes a picture of the scandals and sends it to three friends asking for their opinion. The responses came quickly and were all thumbs up, so Amanda decides to buy the sandals.

This scenario is fictional, inspired by the one in the article entitled "The Future of Shopping"[1] of Harvard Business Review* in its special edition on Consumer Goods & Retail in 2011. However, it could be real. All the technology Amanda uses is already available and within a few years, much of it will be ubiquitous. UltimaModa's virtual consultant uses data from customers stored by the company in the cloud to make recommendations. Social media have created an eco-system where customers talk about brand products. Mobile devices are completely changing the business landscape, extending companies' limits and offering customers almost universal access to information about their products.

As we see in this scenario, information technologies and technological innovation continue to transform the Consumer Goods & Retail industry, bringing new opportunities and challenges for sector CIOs. CompTIA, an IT trade association from the US, conducted a survey last summer among 500 retailers[2], finding that 72% of retailers surveyed rate technology as important to their business. That figure is projected to increase to 83% by 2014. But the study indicates that large numbers of retailers have not yet succeeded in using technology as well as they could or should. Just 7% of retailers report being exactly where they want to be in using technology, while 29% rate themselves as being very close. The compTIA

*References to other documents are provided at the end of this document.

study cited digital signage, social engagement, geo-location services, mobility and payment processing as among the key technology adoption trends.

In this document, we analyze three technologies that are transforming the Consumer Goods & Retail industry: cloud computing, social media and mobile technologies. The information used for the study stems from prior research conducted by Ernst & Young, putting them in the sector context, and joint research carried out between IE Business School and Ernst & Young on the leading companies in the sector in Spain. We look at each technology from the viewpoint of information security, identifying their advantages and the challenges adopting them, and then we put forward a series of recommendations of how CIOs can use the technology securely and confidently. A key, cross-cutting issue is data leakage. We discuss this at the end of the document and recommend a number of steps to mitigate the potential business risks.

2. Cloud computing in *Consumer Goods & Retail*

Driven by pressure to reduce IT spend amid the economic crisis, many companies are seeking assistance outside the organization to become more efficient. They are mostly looking for IT services that require a smaller upfront investment, that use fewer internal IT resources and that cost less to operate. As a result, services based on cloud computing are becoming more widely adopted.

Cloud computing is the new paradigm in which IT or storage resources previously found in the companies' PCs are now leased and managed by third parties[3]. The business model of cloud services providers includes sharing technological infrastructure among several users and managing system performance with virtualization or data migration techniques across a vast number of machines that may be in different geographical locations. Cloud users don't know where their applications or data are, only that they are somewhere "in the cloud."

IT infrastructure sharing generates economies of scale in both hardware and software. Software services can obtain virtually infinite scalability and incremental growth in accordance with customers' needs. Services are usually charged in a standard "pay-as-you-go" model.

The main change in the transition from IT infrastructure developed in-house to the cloud involves the management of service quality and availability through third-party agreements and relationships. Organizations are faced with the need to understand the inter-dependence of their own systems, which have probably taken years, if not decades, to develop, in order to manage processes that combined their infrastructure services with cloud services. They must also consider how that transition to external cloud computing affects business risk, especially with respect to data security, privacy, and availability, and to compliance with regulations and laws.

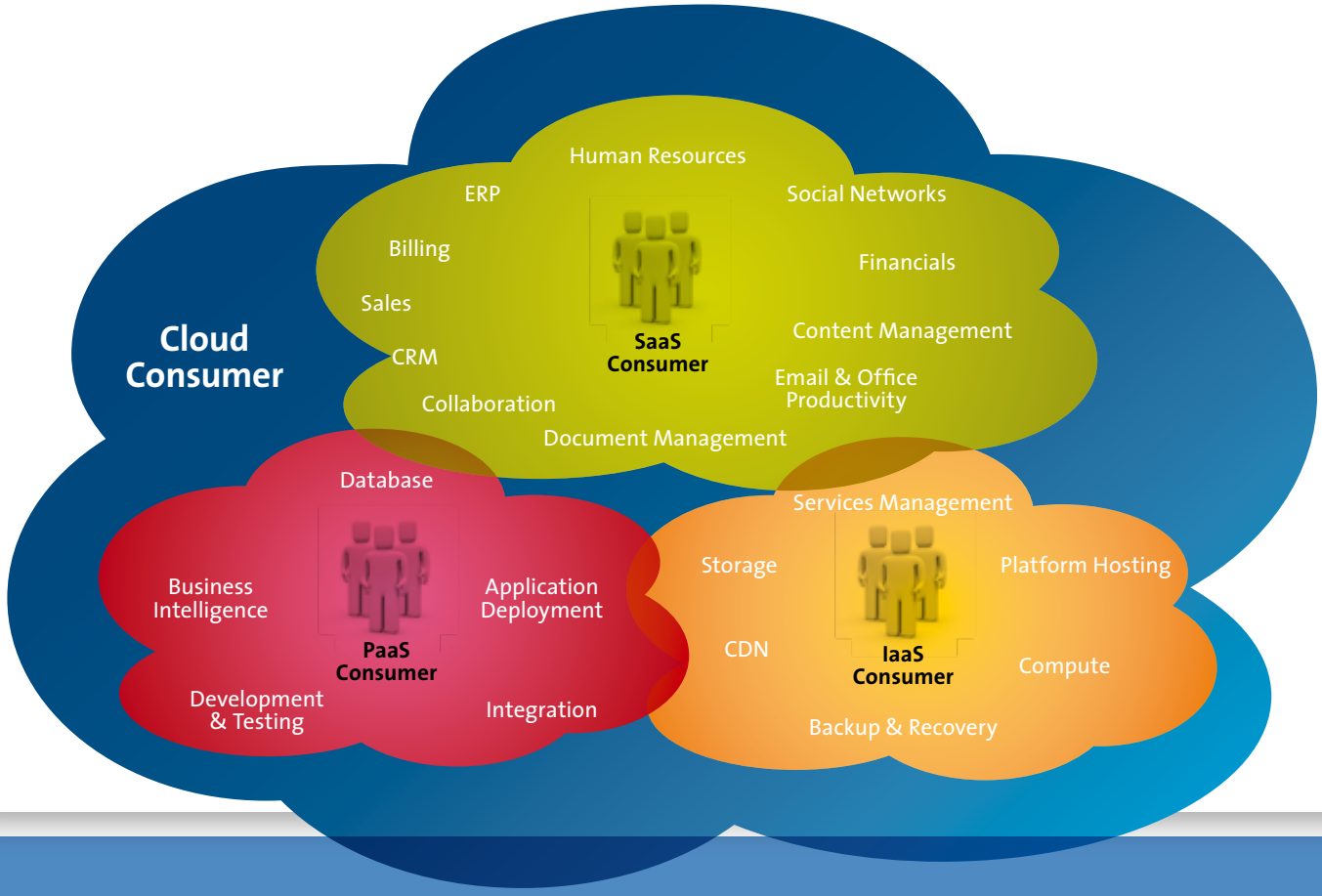
In the context of the Consumer Good & Retail industry, cloud computing is particularly efficient in collection and analyses of huge volumes of sales data and in real time inventory management[4].

sales data and data on consumption patterns of customers can be obtained, for instance, through loyalty cards and coupons and stored on the cloud service provider's network connected to cash registers. Stored data may be accessed from anywhere via Interest, enabling companies to track performance of products, analyze data and identify trends.

To manage their inventory, companies can store real-time data on product sales in numerous stores in the cloud. This makes it easier to obtain data on product availability and analyze data to make realistic forecasts.

The rest of this section deals with the main risks facing companies that want to migrate to the cloud, especially information security and data privacy. We then provide a framework to guide companies in their move to the cloud.

Figure 1: Cloud services models based on NIST (reference 5) *



Cloud computing services are available throughout the IT service spectrum. The Institute of Standards and Technology (NIST) of the US has identified three distinct categories of primary cloud service models[5]:

- **Infrastructure as a service (IaaS):** Computing, storage, and network communication services.
- **Platform as a service (PaaS):** Database, development tools, and other components necessary to support the development and deployment of applications in the cloud.
- **Software as a service (SaaS):** General applications, such as word processing, email, spreadsheet, and specialized applications, such as customer relationship management (CRM) and enterprise resource management (ERM).

**References to other documents are provided at the end of this document.*

It also defines types of deployment models for cloud computing:

- **Private cloud:** The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party, or a combination of both, and may exist on or off the premises of the organization.
- **Public cloud:** The cloud infrastructure is made available to the general public and is owned by an organization selling cloud services.
- **Community cloud:** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, and compliance considerations). It may be managed by one of the organizations or a third party.
- **Hybrid cloud:** The cloud infrastructure is a combination of two or more clouds (private, community, or public).

2.1 Challenges of cloud computing adoption

As with most technological changes, implementing Cloud technology requires considerable changes in traditional technology management methods and business approaches, posing new challenges for CIOs, especially with respect to data security and privacy. These challenges have been identified by a number of organizations and working groups, e.g., Cloud Security Alliance (CSA)[6], National Institute of Standards and Technology (NIST)[7], European Network and Information Security Agency (ENISA)[8], or groups of experts engaged by the European Commission[9].

With the Cloud Computing business model, Cloud service users cannot know exactly where their data are located. This leads to a certain uneasiness among users and lack of trust between users and service providers.

Data privacy is another major area of concern. Personal data stored in the cloud must be handled much more carefully than if it were stored in the company's machines to prevent third-party access from inside the data centers. However, the root of the privacy issue for companies that adopt cloud computing is the diversity of regulations from one country to another regarding privacy. This is particularly worrisome with a model in which the physical location of the data is unknown.

Following we look at the main risks to consider when moving to a cloud computing model based on Ernst & Young's Global Information Security Survey 2011[10].

- **Information security and data integrity.** Processing data with a cloud services provider followed by communication over the internet, as opposed to keeping it within the company network, increases data and information vulnerability. Key information security risks when processing data in the cloud are unauthorized modification to the network's logical or physical areas, unauthorized modification of systems or data and unauthorized deletion of data. A common concern for companies is the loss of control over their business information by trusting cloud providers with secure authentication, user credentials, and data management.

- **Compliance and privacy.** Regarding privacy, a single data breach could cause considerable damage to the name of an organization, hurt its reputation and limit its growth potential, not to mention the direct costs caused by the leak. Organizations are obliged by law or industry regulations to store, trace and even not transfer certain information. Moving data to the cloud does not relieve the organization from its compliance obligations, but rather the contrary. Irrespective of where the data resides, the organization still has its obligations. Accordingly, the organization will need to have a firm grasp of the legal and regulatory requirements of each jurisdiction in which the organization and the cloud provider operate.

- **Standards and interoperability.** Cloud service provides generally develop personalized services that meet the needs of their target public. However, for efficient interaction with the provider's applications, the companies' and the cloud providers' systems need to be able to talk to one another. Otherwise, the continuity of the process, the performance of the application, the inability to tailor applications and the overall efficiency of the desired services are jeopardized. Standards are under development, but this is a lengthy process.

- **Supplier management and governance.** Service level agreements or contracts often stipulate a user's ability to audit a supplier, the legal recourse available in the event of incidents and the owner of the data stored in the cloud. Often they contain essential details regarding key elements of the service; e.g. the level or percentage of availability and the storage space assigned. These terms are often not negotiable, especially for users of basic service packages.

2.2 Recommendations for cloud technology usage

Most security controls are based on standards such as ISO 27001 adapted to the cloud computing model[11]. In Ernst & Young's 2011 Global Information Security Survey, which received feedback from nearly 1,700 participants in 52 countries and across all sectors, including 104 organizations from the Consumer Goods & Retail sector, 52% of those surveyed had implemented no controls to mitigate the risks of adopting cloud technology, while the main control used was merely stronger oversight of the contract management process, which only 22% of those surveyed has implemented (see Figure 2).

In Spain, Observatorio Nacional de las Telecomunicaciones y de la SI (the national telecommunications and information society observatory -ONTSI-) conducted a study recently on the challenges and opportunities of cloud computing[12], especially for Spanish SMEs. Highlights of the survey include that of the 1,700 companies surveyed, 42.5% know what cloud computing is; the main reason for moving to the cloud is the greater flexibility and scalability afforded by the technology; the main benefits perceived are time and costs; and 63.4% of cloud users would recommend the technology without a doubt to other similar companies. By contrast, the greatest concern of those surveyed was security and confidentiality.

Figure 2. Which of the following controls have you implemented to mitigate the new or increased risks related to the use of cloud technology?

As part of the research by IE Business School and Ernst & Young, we set up a working group with representatives of 10 leading companies in the Consumer Goods & Retail sector in Spain. As for cloud computing, all participants recognize the benefits of cloud technology. The companies that have implemented the technology chose the private cloud or hybrid cloud deployment methods.

Governance in the cloud poses many of the challenges in cloud computing adoption through the development of service certification processes, audit frameworks similar to those used in the financial services industry, and the development of reference guides and frameworks explaining how companies can move to the cloud.

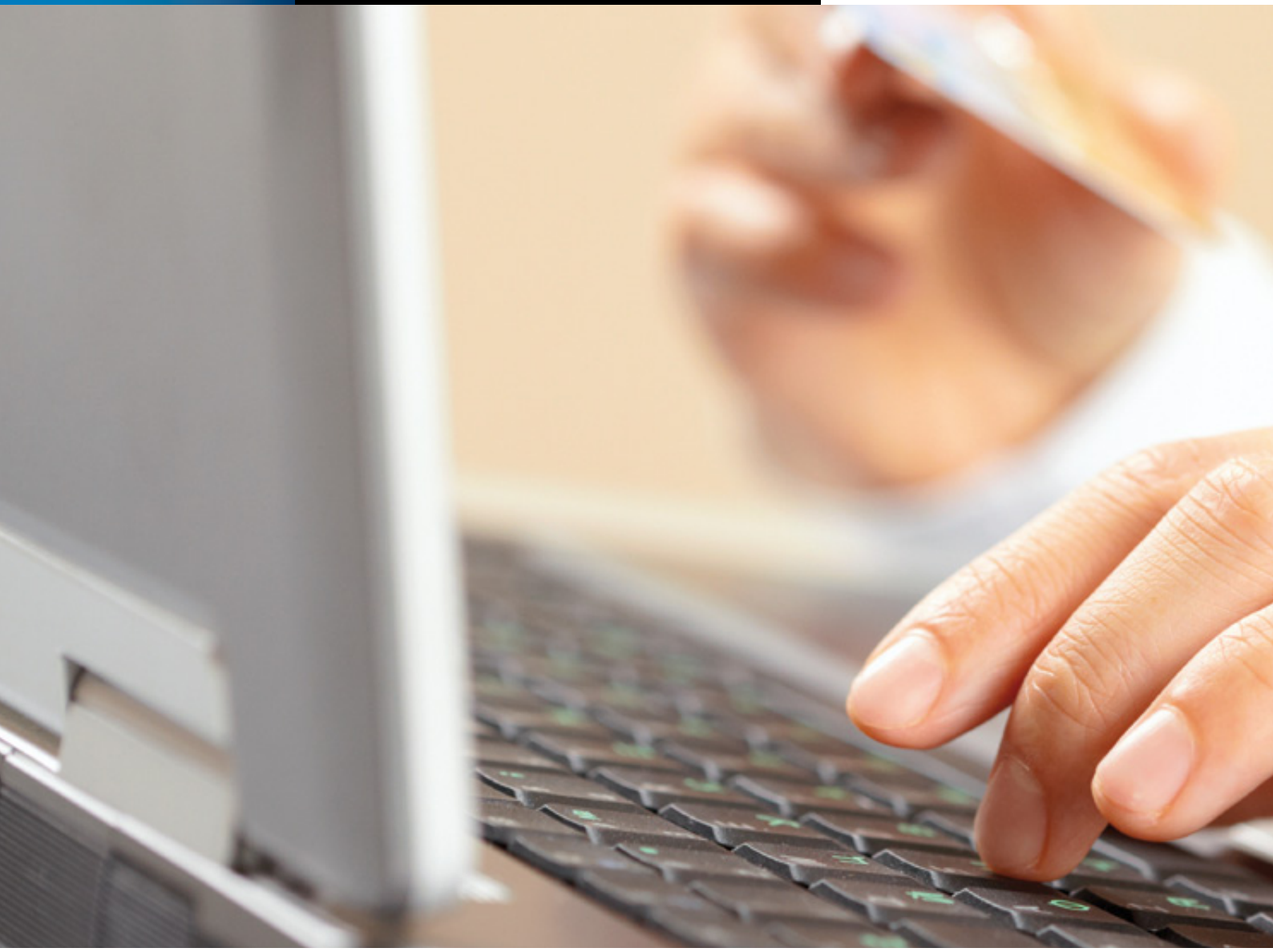
Given the challenges of cloud computing adoption, several organizations promote secure and reliable use of cloud technology; e.g., ENISA in Europe, and CSA and NIST in the US have all begun proposing controls to mitigate the potential risks of adoption of the technology and developing the governance process in the cloud[13].

Below is a summary of the steps to follow when assessing moving to cloud computing in accordance with the reference framework suggested by CSA:

- **Identify the asset for cloud deployment.** The first step in evaluating risk for the cloud is to determine exactly what data or applications are going to be moved to the cloud.
- **Evaluate the asset.** The next step is to assess confidentiality, integrity, and traceability requirements for the asset, determining how risks change for assets in the cloud.
- **Map the asset to the cloud deployment model:** public, private, hybrid or community.
- **Select the cloud service model,** i.e. software, platform or infrastructure as a service, and the cloud service provider.
- **Map out the potential data flow between the organization,** the cloud service and any customers/other nodes.

Our recommendations regarding cloud computing adoption in the retail sector are as follows:

- **Provide clarity to risk management.** The company needs to understand its risk tolerance and who bears the risk when entering into a cloud agreement. Specifically, find out the supplier's policy with respect to security/privacy breaches, and what remedial actions it takes.
- **Choose verification over trust.** Some questions companies should ask themselves are whether the Cloud services provider is certified in accordance with international standards or whether they allow for external audits of the data processing.
- **Draw up a continuity plan** and select providers that are transparent about creating backup copies and testing recoverability in the event of failures.
- **Proceed in using the standard security** processes and techniques that have worked effectively on other technologies in the past.
- **Align your business and information security strategy,** and continuously assess risks to comply with regulations and industry standards.



Case study:
Reliability in the event of a cloud services provider failure

Cloud reliability has been a point of debate until now, with some arguing that it is not as reliable as a well managed local structure. To illustrate, in April 2011, a large part of the Amazon Web Services infrastructure suffered an outage for three days, leaving many companies that relied on the service without access to their applications and data[14].

Figure 3. News of Amazon Web Services outage in 2011 in BBC Mundo

Amazon se disculpa por la caída de su "nube"

Redacción
BBC Mundo
Sábado, 30 de abril de 2011

El gigante de las ventas en internet Amazon se ha visto obligado a pedir disculpas por un problema en su servicio de alojamiento de páginas web EC2 que sacó del aire a numerosos sitios.

El pasado jueves 21 de abril, la interrupción del servicio de Amazon hizo que se cayeran Foursquare, Reddit y Quora, algunos incluso más de un día.

Four Square fue uno de los sitios en internet que cayó por el fallo en los servidores de Amazon.

However, other users of the service knew how to cope with the situation. For instance, Netflix, the online video rental service, was able to continue operating without any problems. Netflix followed Amazon's recommendations and designed an architecture that coped with service interruptions through data and application replication. A key feature of Netflix's system is Chaos Monkey[15], a tool that allows certain applications to be terminated automatically and rebooted in other locations. Amazon's breakdown was serious, but only affected one of its US data centers. By using Chaos Monkey, Netflix was able to cope with the interruption of service at Amazon's data center without any problems and continue providing service with data and applications stored in other centers.

Lessons learned

Analysis of cloud services reliability shows an overall level of 99.9%[16]. This is a fairly high level of reliability that almost certainly would be the envy of many IT departments that process data locally. Given this high availability, it gets a lot of press attention when there are service outages at leading providers.

Netflix has handled the risks of using cloud technology skillfully and has designed solutions to mitigate them. An architecture with redundant systems has been crucial for it to maintain service during provider failures.

3. Social media in the *Consumer Goods & Retail* sector

As internet develops, so does the world of shopping. At first, the web was static and there were just a handful of experts who could create content. In these initial stages, it was merely a channel for companies to promote themselves and sell their products. Nowadays, internet is social, used by millions of people to communicate, talk with friends and share experiences.

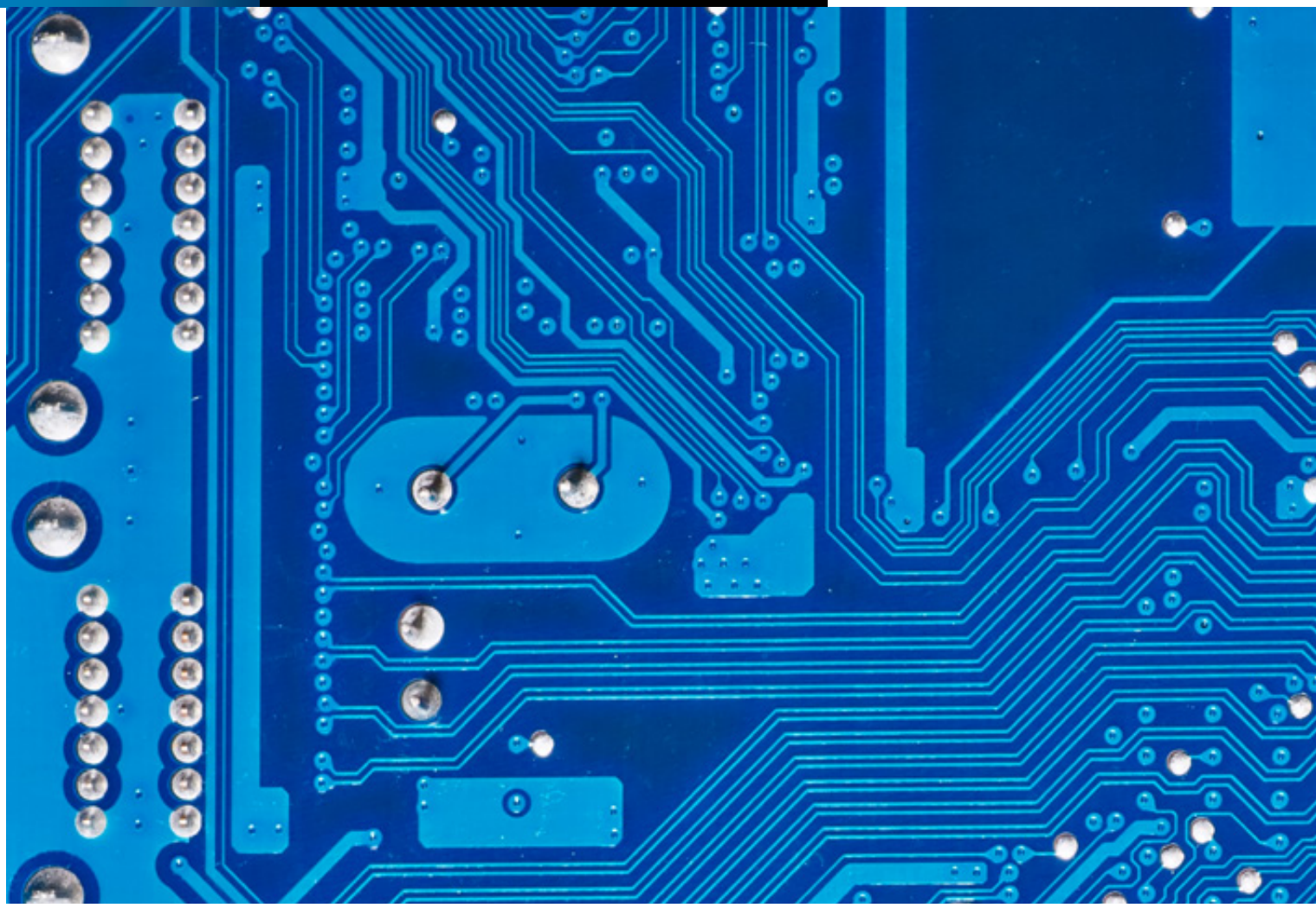
This "social" web opens up huge opportunities for companies. The value of the web economy in G20 countries will nearly double by 2016, according to a report released in January 2012 by Boston Consulting Group17. The study predicts that in four years 3 billion people will be using the internet, almost half the world's population. As for social media, an average of 172 million people visit Facebook every day. Also during the day, 40 million visit Twitter and 22 million visit LinkedIn. More than 860,000 hours of videos are uploaded onto the internet daily and nearly 35 million applications (apps) are downloaded.

Companies can "go social" to create a community, attract new followers of the brand and boost sales. Social media offers a direct communication channel between companies and customers, affording advantages for both. Customers begin to feel like they are part of the company and by feeling like they belong, they are more prone to spend money on the company. By listening to their customers, companies can adapt offers and products to their needs, increasing their propensity to sell.

All of this is having a major impact on the sector. A study on social commerce by JWT Intelligence[18] highlights the impact of social on shopping. According to the study, over 40% of men and more than a third of women are more likely to purchase something if they see that a friend has recommended it on a social network. Similarly, a study by Ernst & Young on social media in the UK in 2011[19] found that two-thirds of those surveyed considered that social media influences their purchases.

In the joint study conducted by IE and Ernst & Young, all companies in the working group agree on the importance of social media for the sector and how it is transforming the way businesses and customers communicate with each other.

Social media not only opens up opportunities. It also poses a great many challenges. Generally speaking, social media is undergoing a similar phenomenon to cloud computing and mobile technologies, whereby limits placed on companies are disappearing and challenges are arising, such as the inadvertent leakage of sensitive corporate data caused by the participation of users in social media or damage to the organization's reputation caused by negative comments of employees or customers.

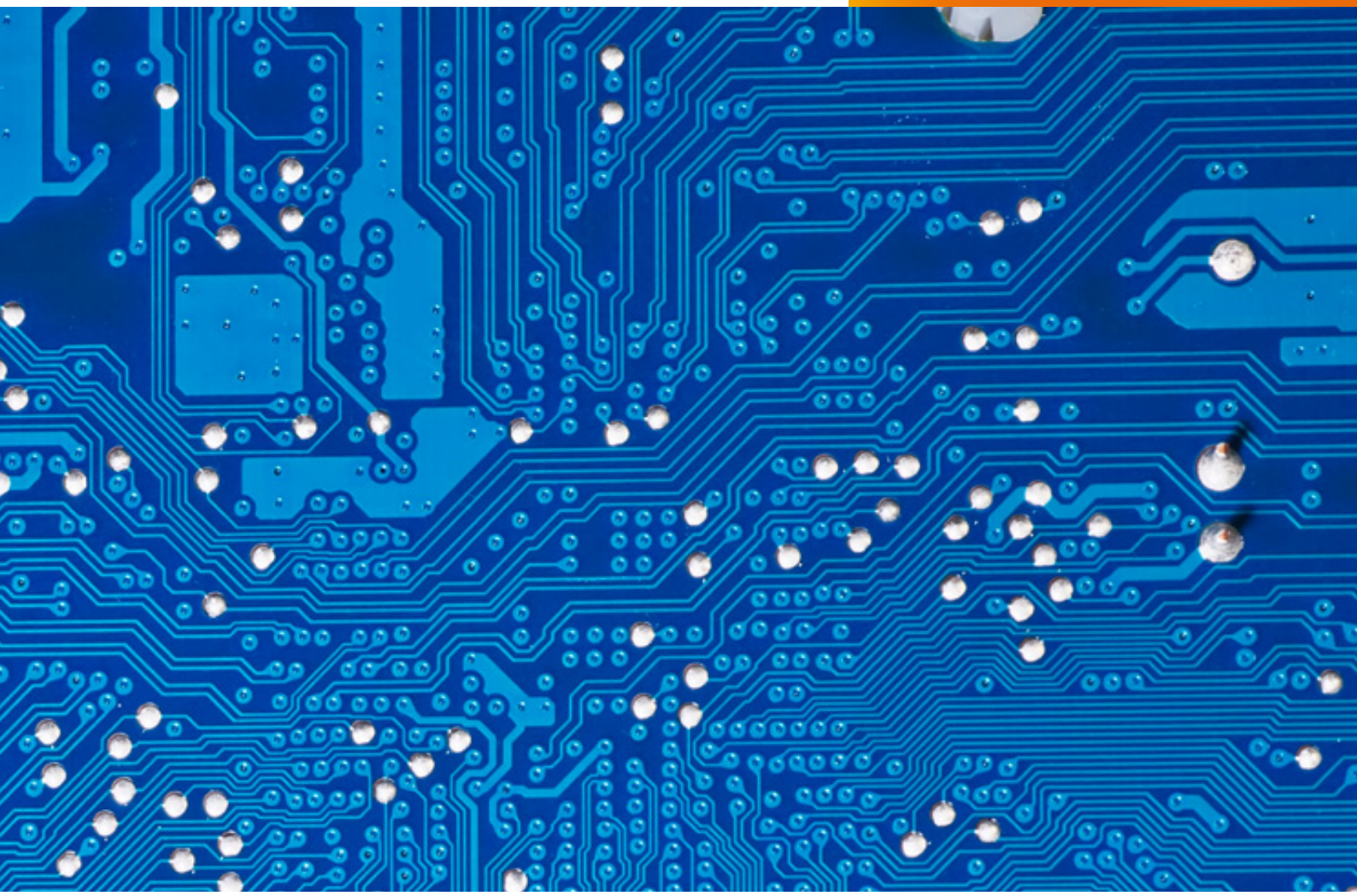


3.1 Understanding the risks of social media

Before, companies created an image for customers and designed products to meet their needs based on transaction data (e.g. purchasing history). With social media, they now have access to new, external data to increase the amount of information on customers and, therefore, can offer more bespoke products.

However, the transformation caused by social media implies changes in how companies approach customers. It has gone from one-way communication to a two-way conversation with customers. As a result, businesses have a new way to engage customers and forge new relations.

Meanwhile, companies have a responsibility to the information that flows in social media. Companies have no control over consumers' opinion, and information can appear that they do not consider for general use or that affects their reputation. Organizations must be able to use social media to engage unsatisfied and critical customers in order to correct mistakes and address concerns head-on and publicly.



Based on a recent study by Ernst & Young entitled "Protecting and strengthening your brand"[20], we have identified the following social media risks:

- **Reputational risks,** such as damage to a brand or company reputation from negative employee or customer posts, even those that are well-intentioned. • Data leakage risks. For instance, employees involved in social media inadvertently leaking sensitive company information.
- **Security risks..** There has been a rapid spread of criminal hackers "re-engineering" confidential information (e.g. log-ins and passwords) through deceit. Also, the number of viruses and malware for social media are on the rise.
- **Data leakage risks.** For instance, employees involved in social media inadvertently leaking sensitive company information.
- **Operational risks,** e.g., employee misuse of social applications while at work.
- **Compliance risk,** failure to retain and record information shared on social media where required by regulations.

Openness and transparency are expected of companies that participate in social media. Organizations that manage risks by ignoring the posts of customers or restricting their participation in social media are making a mistake and the problems can grow exponentially. Collaboration and empowerment are the new currency in social media.

Some companies respond to specific social media-related challenges quickly by enacting piecemeal solutions. This approach frequently results in lost time, energy and money as companies are then forced to react to other issues not originally addressed. We believe companies should build a holistic, enterprise-wide social media strategy that encompasses all efforts to protect and strengthen the brand and that is robust and flexible enough to accommodate constantly changing technological advances.

Based on the digital liability model developed by Volonino and Robinson[21], which included recommendations in prior research by Ernst & Young[22], our recommendations for protecting the brand in social media are as follows:

- **Design a social media protection strategy that has executive support.** A security program needs the support of executives to be successful. The same is true for protecting the brand: executives must have a clear understanding why the organization is in social media and what the advantages are for the business. It is crucial that executive show the organization's commitment to the strategy to encourage other employees to get involved.
- **Analyze the risk of using social media.** Map out the potential risks. Analysis should be enterprise-wide as well as focus on the specific use of social media in different departments.
- **Draft social media policies and guidelines.** Policies and strategy must be compliant with national and international rules and regulations. It is important to carry out campaigns to increase employee awareness of policies and guidelines and the role of employees in the social media strategy.
- **Design a social media monitoring strategy,** including mechanisms to leverage customer insights and lesson learned from social media monitoring.
- **Define a social media incident** response process focused not only on customer feedback and interaction, but also on IT-related security and private-related issued.

Case study:
Hacking of a CEO's twitter account

Best Buy is an international electronics product retailer, with more than 1,400 stores, over 160,000 employees and nearly 50 billion in annual revenues, and is the 11th largest online retailer in the US[23].

Brian J. Dunn was CEO at Best Buy between April 2009 and April 2012. He is now a firm user of social media and convinced of its advantages for the business. Dunn used the corporate blog, Twitter and Facebook to interact with both customers and employees. In an article published by Harvard Business Review24 he said: "I believe that Best Buy's message has to be where people are. Today, that means being on social networks."

Dunn was a particularly avid user of Twitter, with over 5,000 followers. He says, "Twitter is a way to let people know what's on my mind... I tell my employees about good things I see in a store or good experiences with customers. The employees are happy and know I'm hearing good things about them."

In 2010, Dunn's Twitter followers were surprised when they saw a strange message: "I'VE BEEN HAVING A LOT OF GREAT SEX LATELY, AND HERE'S WHY." It was followed by a link to a website, presumably offering male enhancement pills. Obviously, his Twitter accounted had been hacked.

Dunn admitted that, like many people, he had been using a password that was easy to remember and discover because it was based on something in his life.

Figure 4. Dunn's TWITTER accounts as the CEO of Best Buy

Lessons learned

With the help of his IT team, Dunn set up his Twitter account again, selecting a well-constructed password that he changes regularly, in line with company policy.

Important: the negative experience did not stop Dunn from continuing to use social media. He said, "You can't use them [social media] only when things are good. You have to deal with rain as well as sunshine."

4. Connecting in a mobile world

Over the past few decades, we have witnessed significant technology advance in mobile devices, from the personal data assistants (PDAs) of the late 1990s to the ubiquitous smartphones and tablets of today. These advances have extended the virtual boundaries of the enterprise, blurring the lines between home and office. At the same time, the so-called "m-commerce" –mobile commerce- is growing rapidly. To illustrates, recent studies in the North American market show that 25% of mobile users shop online via a mobile device[25]. In Spain, a recent study by ONTSI[26] indicates that 9% of internet users have made a purchase using their mobile device. These rates are likely to rise now that the devices are becoming more popular.

For businesses, mobile devices permit constant access to email and business applications. This has prompted some organizations to redesign their business models and develop new applications. Mobile devices have also allowed access to, and storing of, potentially sensitive company data[27]. Companies must be aware of the risks that come with these changes.

At the same time, another huge change is taking place in organizations. A large number of companies are providing technical support and access to their applications from employees' own mobile devices, known as "bring your own device" - BYOD[28]. This concept also has new risks. For instance, an employee may inadvertently lower the security of their own mobile device, opening it up for potential attacks.

In short, greater access to information has led to increased productivity, but it has also increased information security risks. Therefore, companies need to identify the potential risks, and define effective strategies and adopt measures to deal with them.

In the Consumer Goods & Retail sector, consumers are taking advantage of the large number of channels and devices that enable them to make purchases any time, any where and faster than ever, as seen by the growing number of apps for smartphones that make shopping faster and easier. Changes will continue to take place rapidly in the years ahead and the sector needs to be ready to meet the expectations of consumers and their demand for a faster, easier, and more personalized shopping experience.

4.1 Mobile device risks

The ubiquity of mobile devices in the corporate environment has allowed the further expansion of the corporate office. From a security perspective, the risks and potential effects of deploying and supporting mobile devices as a corporate tool must be understood. Following, we present the main risks related to mobile devices according to a study on mobile device security carried out by Ernst & Young29 and SearchSecurity.com[30].

- **Stolen or lost devices.** A fundamental problem with mobile devices is physical access control. By their design, mobile devices are most useful outside of the office and on the move with the owner. This presents several concerns for a security administrator, as the device on the move is more likely to be lost or stolen — and subsequently used by a malicious attacker.
- **Policy implementation.** Compared to laptops, mobile devices often contain stronger client-side controls that can be altered, which can pose security problems. For instance, device locking can be changed or the device can be used as a modem. This would bypass some device restrictions and allow a malicious user to attack the internal network more easily. In addition, owners may bypass device restrictions through a method known as "jailbreaking," after which they can remove any policy requirements on the device, install unapproved applications, and potentially be exposed to additional security threats.
- **Malicious software from applications.** Mobile devices mainly access business software and data through applications that can either be acquired from software stores or provided by the company. There is a risk of installing malicious software on the device. Recently, app stores, like Google Play, have had to apply stricter selection criteria because of the increasing number of malware[31].

4.2 Mobile device security recommendations

Following, we put forward some security recommendations for mobile device usage in organizations based on recommendations presented in other studies.[32, 33]

- **Create and implement IT policies that govern usage of mobile devices.** The policies should define how to keep information private, and define ownership of the data and applications on the devices. Establish awareness programs so that all employees know and understand the policies.
- **Implement mobile device security.** All mobile devices should be password-protected; limits should be placed on sensitive data transferred to mobile devices or view-only access should be considered. It is important to assess utilizing mobile device management software that guarantees encrypted connection for sensitive data. We also recommend training application developers in secure coding practices for mobile device platforms.
- **Create a mobile device security working group.** The group should perform technical security assessments on mobile devices and the supporting infrastructure, as well as evaluate new and emerging threats. Another recommendation is to add mobile security to existing employee security awareness programs.

Case study:
When a free app becomes expensive

A food storage chain was hit with a security breach. The worst part of the breach was that the chain had no idea how it happened. It was not until the digital crimes unit of the police went to one of the stores that the company found out that it had even suffered an attack.

The fraud was uncovered from when bank branches in different parts of the country began receiving phone calls from customers complaining that their credit cards had been charged for purchases they had not made. The banks called the police and all the evidence pointed to some type of data capture during credit-card transactions at several stores in the chain.

The managers' first reaction was to assume that the fraud came from somewhere else, because the company followed standard industry procedures regarding credit-card payments. Nonetheless, the company cooperated with the police in their investigations.

The police inspected the transaction records of several stores and found malware installed on the information management system at the points of sale. The software was a packet sniffer[34] that "sniffed" the POS' outgoing data and captured the credit card information before it was eliminated from the device and the company's servers which, according to industry standards, should happen immediately once bank authorization is received. Since the malware was a personalized code, it went undetected by virus scans and other similar software. Much to the company's surprise, the malicious software was found at each store.

But, how did the software get installed on the company's systems? In the forensic analysis, the access logs showed that the software had been installed immediately after some employees had accessed corporate transactions from their mobile devices. The company had updated its ERP system a year before and the update allowed mobile access to the corporate systems. Not all employees had access, but certain mangers had requested it. They were given temporary access by the IT department from both corporate and personal devices. After performing checks on the devices, it turned out that one manager had installed a free, unauthorized version of a popular game. Hackers used the application to access the other devices to which the user was connected and install the malicious software.

Lessons learned

Several lessons can be learned from this story. First, the company thought that by complying with industry standards for credit-card payments, it was ensuring the security of its payment system. Industry standards such as PCI-DSS are excellent indicators of information management quality, but not a guarantee of security for the company's assets[35].

BYOD obviously gives companies advantages despite the potential security risks[36]. Companies need to define clear policies for usage of mobile devices and find ways to ensure the security of all the users' devices. Extremely important is that they carry out security awareness programs

Data loss

Over the last few years, companies in every sector around the globe have seen their sensitive internal data lost, stolen or leaked to the outside world. A wide range of high-profile data loss incidents led to millions in direct and indirect costs for companies and have resulted in tremendous damage to brands and reputations.

Many different types of incidents have occurred, including the sale of customer account details to external parties and the loss of many laptops, USB sticks, backup tapes and mobile devices, to name just a few. The vast majority of these incidents resulted from the actions of internal users and trusted third parties, and most have been unintentional.

As data is likely one of your organization's most valuable assets, protecting it and keeping it out of the public domain is of paramount importance. One technique is DLP (Data Loss Prevention), a set of products and strategies to help companies protect their information[37]. DLP is not a standalone product like a firewall. It consists of a set of technologies designed to prevent data loss by identifying sensitive data, monitoring activity, and blocking data from moving from one place to another if pre-defined rules are broken.

However, before DLP controls can be effectively implemented, organizations must understand the answer to these three fundamental questions:

- What sensitive data does the company hold?
- Where does sensitive data reside, both internally and with third parties?
- Where are the data going and what is the data flow in the company?

5.1 Challenges of data loss management

The information derived from data is any organization's most valuable asset. A number of high-profile data leakage events have recently brought this issue into the public eye.

With the emergence of cloud technology, the data loss threat has grown rapidly. The increased amount of data that is carried around through the use of mobile devices heightens the risk that unauthorized parties can gain access to sensitive data.

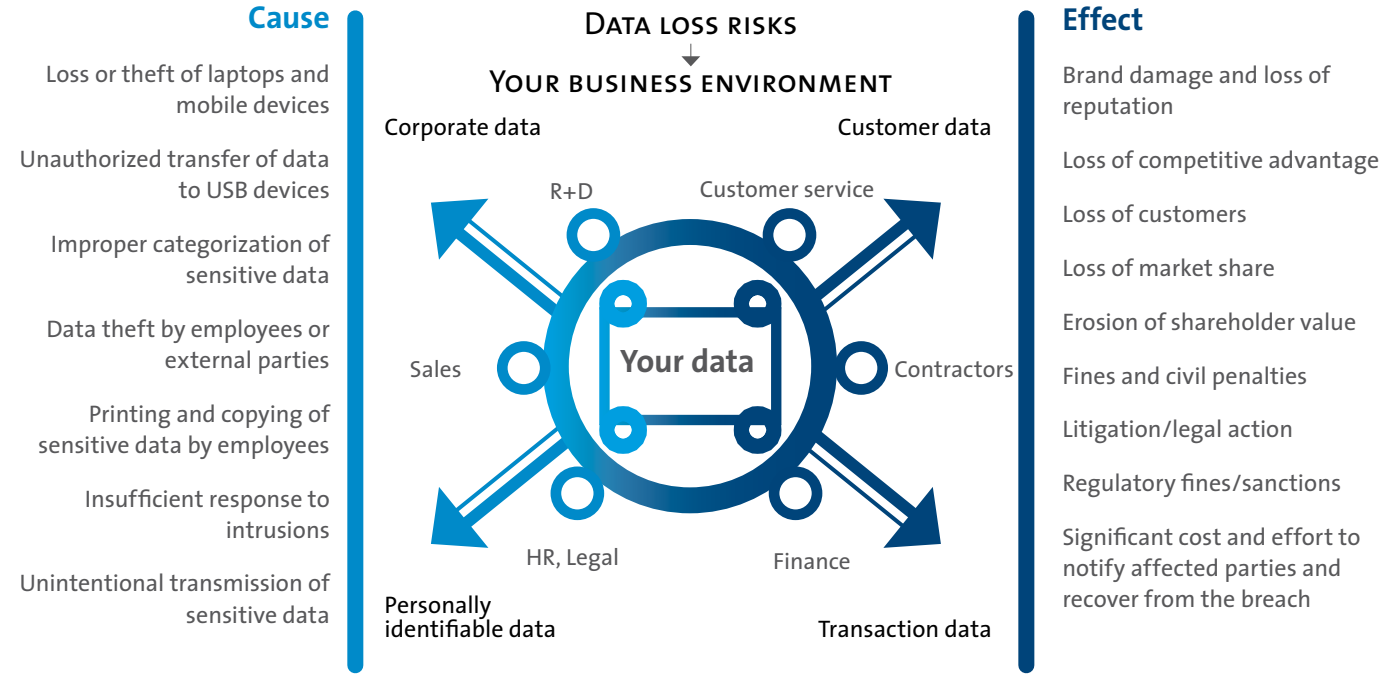
But data loss is not only limited to the risk of physical loss of devices, such as tablet computers, mobile phones or laptop computers. Many incidents are also due to accidental disclosure through electronic transmissions or in social media. In most cases, employees are not even aware of the risks associated with sending sensitive data through unencrypted emails, instant messages, webmail or file transfer tools.

Holes through which data can leak are made larger by the use of decentralized systems and work collaboration tools, making it even more difficult for organizations to track and control information.

Another complicating factor in efforts to help control data is the availability of increasingly inexpensive storage devices. Many gigabytes of data can literally "walk" out the door on an employee's keychain or in a smartphone, or they can be intercepted when sent through a low-cost cloud service.

In managing data loss, there are so many reasons why data loss can occur, numerous data loss scenarios to account for and many different controls that must be effective in order to manage the problem[38]. To address the issue, a comprehensive solution that includes people, processes and technology needs to be implemented (see Figure 5).

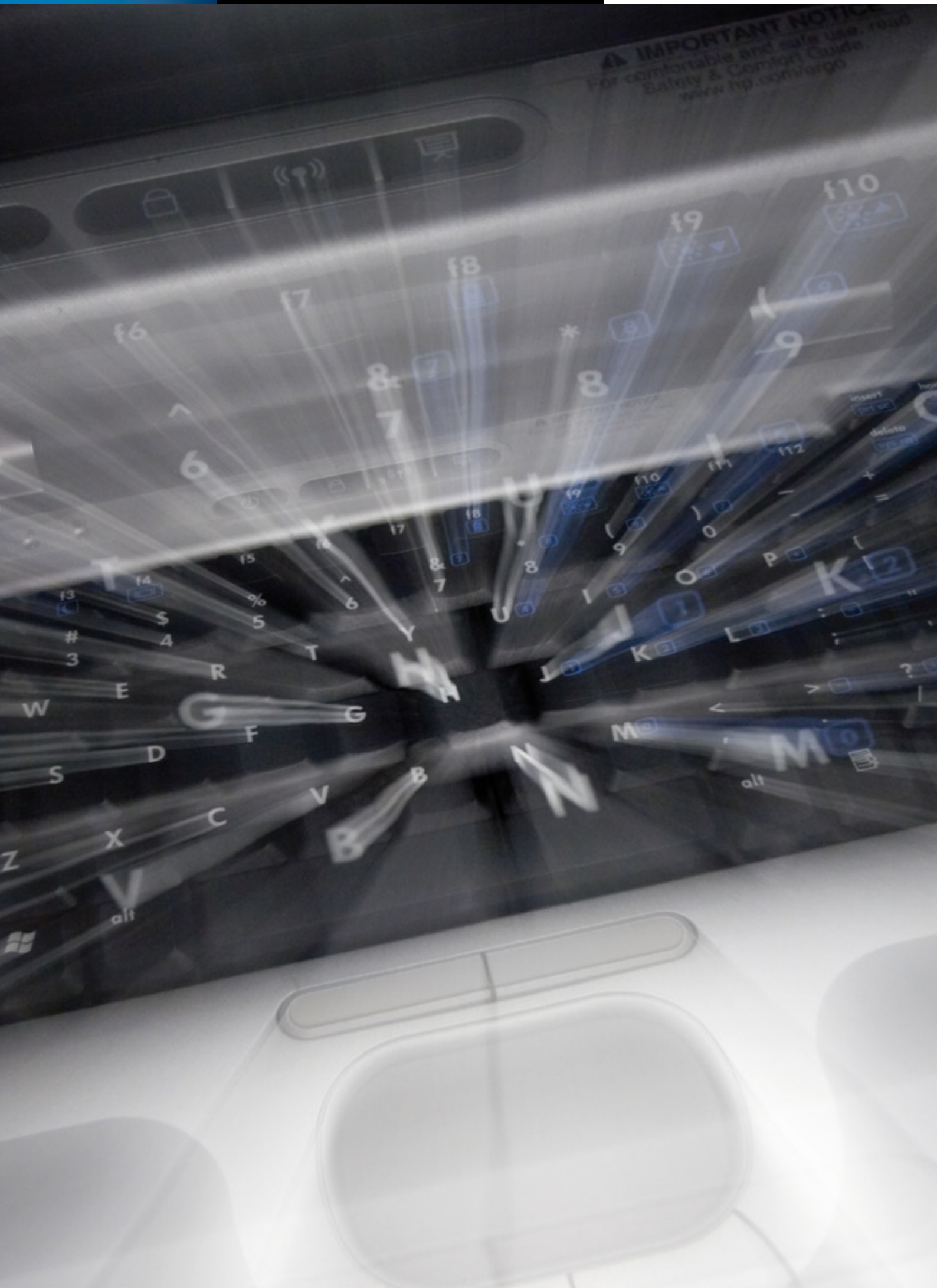
Figure 5: Causes and effects of data loss in the corporate environment. Adapted to the Ernst & Young report Data Loss Prevention (reference 39).



Following we offer some tips for managing data loss based on previous research [40, 41]:

5.2 Recommendations for managing data loss

- **Identify, assess, and classify sensitive** data across the enterprise so that DLP controls can be focused to provide protection for the organization's most sensitive data.
- Assess, understand, and appreciate the many potential risks and areas of data loss, specifically **documenting and ranking the risks relating to the data loss channels** in the company.
- **Identify key DLP controls and measure their effectiveness.** All key controls that support the data loss prevention program, such as asset management and physical security controls, should be understood to provide accurate reporting of data loss risks and controls.
- **Understand what data is sent to third parties, how it is sent and if the transmission mechanisms are secure.** Organizations have a responsibility to perform due diligence to validate that third-party data stewards have reasonable safeguards in place for protecting sensitive company data.
- **Cover data in motion,** data at rest and data in use within the organization's DLP controls.
- **Implement incident investigation,** enlist a strong team to carry out the program and seek the support of key stakeholders throughout the business to create a successful DLP program.


IMPORTANT NOTICE
For comfortable and safe use, read
Safety & Comfort Guide
www.hp.com/ergo
f10
f9
f8
f7
f6
alt

Case study:
TJX data breach

TJX was the largest apparel and home fashions retailed in the US in the off-price segment. TJX ranked 138th in the Fortune 500 rankings for 2006. With US$17.4 billion in sales for the year ending January 2007, the company was triple the size of Ross Stores Inc., its closest competitor.

It was on December 18, 2006, that the company learned of hacking. The presence of suspicious software, altered computer files and mixed-up data were among the first evidence of the intrusion. Involving the segment of the computer network handling payment cards, checks, and merchandise return transactions for customers, it seemed to affect all the eight businesses of the company and all the stores in the US, Puerto Rico, Canada, and the UK.

In March 2007[42], TJX said 45.6 million credit and debit card numbers were stolen from one of its systems over a period of more than 18 months by an unknown number of intruders.

In addition, personal data provided in connection with the return of merchandise by about 451,000 individuals in 2003 was also stolen. By October[43], the number of cards affected had doubled to nearly 94 million, with estimated losses for banks of between US$68 million and US$83 million.

But how did the intrusion at TJX really happen? Based on the scale of the intrusion, IT experts believed there were multiple points of attack. Investigations indicated that the company's encryption techniques were weak, allowing the intruders to decrypt the information. The Wall Street Journal[44] reported that the theft began in 2005 through a wireless network at one of TJX's Marshall stores. Meanwhile, Information Week[45] considered that another means of attack was through social engineering, with attackers posing as prospective job applicants with TJX and accessing the equipment of the employment application kiosks, where they installed the malicious software they had on USB drives.

Lessons learned

TJX suffered huge economic losses and damage to its reputation. A year after the breach, the company estimated that it had cost US$250 million[46].

Investigations showed that the company stored customer data that it did not need, such as that found on the magnetic strips of the credit cards. TJX did not have any controls in place to prevent its leakage. In addition, the company had not set up security controls in accordance with industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS).

This case illustrated that the company had a lot of work ahead of it and needed to change its approach to IT security. TJX began by reviewing its main risks and designing strategies to mitigate them to prevent a similar intrusion from happening again. Mid term, it needs to view information security as not just a technical issue, but rather a factor with a considerable impact on the business and requiring the involvement of all company staff.

6. Ernst & Young viewpoint

The story of Amanda presented in the introduction is fictional, but the situations described and the interaction between customers of Consumer Goods & Retail companies with cloud computing, social media, and mobile devices are real. Because of these new technologies, companies are becoming increasingly vulnerable to data leakage of sensitive business information.

The benefits of cloud computing, the need to have presence in social media and the advantages of using mobile devices concern all industries, but perhaps affect Consumer Goods & Retail companies the most as they are forced to adopt the changes or be left in the wake of their rivals.

To remain competitive, most sector companies are faced with the issues presented in this research, either because they are making the change or because they intend to do so in the near future.

Many of these companies are faced with the decision of how to address, technologically, the changes in social behavior from a security viewpoint. They need to know the risks to which they are exposed and, in order to mitigate them, how to deal with the changes taking place in their business models.

This report attempts to provide some insight into processes we find each day with sector customers committed to tackling the technological challenges with the required level of security and exploiting the business opportunities the new trends are creating for them.

RAMIRO MIRONES GÓMEZ

Partner Ernst & Young

Ramiro Mirones has 14 years' experience at Ernst & Young performing IT system audits and consulting projects on compliance with IT security and internal control requirements. He has participated in audits related to the Sarbanes-Oxley Act, section 404.

He currently Head of Consumer Goods & Retail, and Telecommunications in the IT Risk and Assurance Services (ITRA) department. Clients include major Spanish and US enterprises. He is also in charge of the ERP Skill Center in Spain.

He is a graduate in Business Administration and Management from Universidad de Valladolid, and holds a BA in Economics & Statistics (European Studies) with Honors from the University of Exeter and an Executive MBA from IESE Business School.

References

1 D. Rigby. The Future of Shopping. Harvard Business Review, Vol 89, Issue 12, December 2011

2 CompTIA. Retail Sector Technology Adoption Trends Study. compTIA, the IT Industry Association. Junio 2012.

3 M. Armbrust, et al. Above the Cloud: A View of Cloud Computing. Communication of the ACM 53 (4), 50-58, 2010.

4 Fibre2fashion.com. The Future of Retail Industry is in Cloud Computing. Agosto 20, 2010. http://www.fibre2fashion.com/industry-article/29/2883/the-future-of-retail-industry1.asp

5 F. Liu et al. NIST Cloud Computing Reference Architecture. NIST Special Publication 500-292. September 2011.

6 CSA. Top Threats to Cloud Computing V1.0. Cloud Security Alliance, March 2010. Disponible en https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

7 NIST. Guidelines on Security and Privacy in Public Cloud Computing. NIST, December 2011. Disponible en http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909494.

8 ENISA. Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información. ENISA 2009. Disponible en http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/view.

9 EU. The Future of Cloud Computing: Opportunities for European Cloud Computing Beyond 2010, European Commission, 27 January 2010.

10 Ernst & Young. Into the cloud, out of the fog. Insights on IT risk. Business briefing, November 2011.

11 K. Julisch, M. Hall. Security and Controls in the Cloud. Information Security Journal, A Global Perspective. Volume 19, Issue 6, 2010.

12 ONTSI. Cloud Computing – Retos y Oportunidades. Observatorio Nacional de las Telecomunicaciones y de la SI – ONTSI. Mayo 2012. Disponible en http://www.ontsi.red.es/ontsi/es/estudios-informes/cloud-computing-retos-y-oportunidades.

13 Security Guidance for Critical Areas of Focus in Cloud Computing. V3.0. Cloud Security Alliance, 2011.

14 Amazon. Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region. http://aws.amazon.com/message/65648/.

15 K. Finley. Chaos Monkey: How Netflix Uses Random Failure to Ensure Success. December 2010. http://readwrite.com/2010/12/20/chaos-monkey-how-netflix-uses.

16 M. Gagnaire et al. Downtime statistics of current cloud solutions. IWGCR: The International Working Group on Cloud Computing Resiliency, 2012. http://iwgcr.org/wp-content/uploads/2012/06/IWGCR-Paris.Ranking-002-en.pdf.

17 Boston Consulting Group. The Internet Economy in the G-20: The $4.2 Trillion Growth Opportunity. 2012.

18 JWT Intelligence. Social Commerce. July 2011

19 Ernst & Young. YouGov Social Media Survey. 2011.

20 Ernst & Young. Protecting and strengthening your brand. Insights on IT risk, Business briefing. May 2012.

21 L. Volovino and S. R. Robinson. Principles and Practice of Information Security. Pearson Prentice Hall, 2004.

22 Ernst & Young. Op cit 20. Protecting and strengthening your brand.

23 About Best Buy. http://pr.bby.com/about-best-buy/

24 B. J. Dunn. How I Did It ... Best Buy's CEO on Learning to Love Social Media. Harvard Business Review, December 2010.

25 C. Tode. 25pc of mobile users shop online only via a smartphone or tablet. Luxury Daily, July 9 2012. http://www.luxurydaily.com/25pc-of-mobile-users-shop-online-only-via-a-smartphone-or-tablet-study/.

26 ONTSI. Comercio Electrónico B2C 2011. Observatorio Nacional de las Telecomunicaciones y de la SI –ONTSI. October 2012. http://www.ontsi.red.es/ontsi/es/estudios-informes/estudio-b2c-2011 edici%C3%B3n-2012.

27 M. Satyanarayanan. Mobile Computing: The Next Decade. Proceedings of the ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond (MCS), ACM, 2010

28 T. Bradley. Pros and Cons of Bringing Your Own Device to Work. PC World, December 20 2011. Disponible en http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html .

29 Ernst & Young. Mobile device security. Insights on IT risk. Technical briefing, January 2012.

30 SearchSecurity.com. Enterprise Mobile Security Survey 2012. http://searchsecurity.techtarget.com/guides/Survey-Enterprise-mobile-device-security-2012.

31 BBC News. Android hit by rogue app malware. March 2011. http://www.bbc.co.uk/news/technology 12633923.

32 Ernst & Young. Op. cit 29. Mobile device security.

33 Webroot. Mobile Security Decision-Makers Report BYOD Threats Have Infiltrated Their Organizations November 2012. http://www.darkreading.com/mobile-security/167901113/security/news/240124947/mobile-security decision-makers-report-byod-threats-have-infiltrated-their-organizations.html

34 T. Bradley. Introduction to Packet Sniffing. http://netsecurity.about.com/cs/hackertools/a/aa121403.htm.

35 Infosecurity. PCI-DSS compliance does not always guarantee security. Infosecurity magazine, August 07 2009. http://www.infosecurity-magazine.com/view/3094/pcidss-compliance-does-not-always-guarantee-security/.

36 W. Ashford. Nearly half of firms supporting BYOD report data breaches. ComputerWeekly.com, August 9 2012. http://www.computerweekly.com/news/2240161202/Nearly-half-of-firms-supporting-BYOD-report data-breaches.

37 CSO. The Executive Guide to Data Loss Prevention. CSO Magazine, CSO Executive Guide, Summer 2010.

38 S. Liu, R. Kuhn. Data Loss Prevention. IT Pro, IEEE Computer Society, March/April 2010.

39 Ernst & Young. Data loss prevention. Insights on IT risk. Business briefing, October 2011.

40 Ernst & Young. Op. cit 40. Data loss prevention.

41 ComputerWeekly. Top Seven Data Loss Issues. ComputerWeekly.com, 2009. Disponible en http://www.computerweekly.com/feature/Top-seven-data-loss-issues.

42 J. Vijayan. TJX data breach: At 45.6M card numbers, it s the biggest ever. Computerworld, March 2007. http://www.computerworld.com/s/article/9014782/TJX_data_breach_At_45.6M_card_numbers_it_s_the_biggest_ever.

43 R. Kerber. Court filing in TJX breach doubles toll. The Boston Globe, October 24 3007. http://www.boston.com/business/globe/articles/2007/10/24/court_filing_in_tjx_breach_doubles_toll/.

44 J. Pereira. How Credit Card Data Went Out Wireless Door. The Wall Street Journal, May 4 2007. http://online.wsj.com/article/SB117824446226991797.html.

45 K. Jackson Higgings. Hacking the Real TJX Story. Information Week, online edition, March 15 2007. http://www.informationweek.com/security/government/hacking-the-real-tjx-story/208803414?queryText=TJX.

46 J. Vijayan. One year later: Five takeaways from the TJX breach. Computerworld, January 17 2008. http://www.computerworld.com/s/article/9057758/One_year_later_Five_takeaways_from_the_TJX_breach?taxonomyId=82&pageNumber=1.

vv

ie foundation

The IE Foundation is an instrument of IE that enables students, teachers and staff to further their educational, research and management activities.

Priority is given to the training and cultural outreach of all people and institutions that have ties with IE.

Resources go to funding scholarships for students, grants for training and research for professors, and funds for updating and improving IE's educational structure.

The Foundation operates throughout Spain, but also has an international presence throughout North and South America, Southeast Asia, the Middle East, Northern Africa and Europe.

www.ie.edu
fundacion.ie@ie.edu

ERNST & YOUNG
Quality In Everything We Do

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 167.000 people are united by our shared values and an unwavering commitment to quality. we make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst &Young Global Limited, a UK company Limited by guarantee, does not provide services to clients. For more information about our organization, please visit

www.ey.com