KPMG

2001 GLOBAL e.fr@ud.survey

KPMG FORENSIC & LITIGATION SERVICES


“AS E-COMMERCE
REVOLUTIONIZES
BUSINESS, IT ALSO
REVOLUTIONIZES
BUSINESS FRAUD.”

Contents

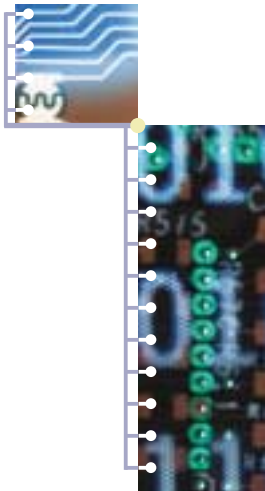
EXECUTIVE BRIEFING

As e-commerce revolutionizes business, it also revolutionizes business fraud. KPMG surveyed the world's largest companies in 12 countries on the topics of e.fr@ud and security-related issues, revealing the following:

- Sixty-two percent of survey respondents have embraced e-commerce in their business, which may include business-to-business, business-to-consumer, consumer-to-business, and/or web page exposure.
- Only 9 percent of respondents indicated that a security breach had occurred in their organization within the last 12 months. Although the reported number of instances of e.fr@ud and security breaches were low, e.fr@ud is a growing problem for companies around the world. Where breaches had occurred, legal action was not always pursued for a variety of reasons, including inadequate legal remedies and a lack of evidence. The existence and use of good computer forensic response guidelines could significantly increase the likelihood of an organization securing the evidence necessary to pursue legal action and/or the recovery of misappropriated assets.
- Respondents indicated overwhelmingly that security of credit card numbers and personal information were by far the most important concerns to their customers. However, less than 35 percent of respondents reported having security audits performed on their e-commerce systems. Only 12 percent of respondents reported that their web site bears a seal identifying that their e-commerce system had passed a security audit.
- Fifty percent of businesses identified hackers and the poor implementation of security policies as the greatest threats to their e-commerce systems. Seventy-nine percent of respondents stated that the highest probability of a breach occurring to their e-commerce system would be perpetrated through the Internet or other external access. However, it is well documented that a company is at greater risk of being the victim of an internal security breach. The survey results illustrate how executives can be misinformed about the actual vulnerabilities of their network systems. Poorly trained and/or poorly qualified system administrators, poor reporting procedures for security breaches, or dishonest employees are often the cause of this misinformation.

- One-half of respondents stated that their organization has incident response procedures to deal with security breaches of their e-commerce system. Of those respondents who have incident response procedures, only 43 percent (or 22 percent of the total respondents) include computer forensic response guidelines.
- Survey respondents from the majority of the participating countries stated that the security of their e-commerce system could be most improved by regular system penetration testing (authorized hacking), the use of software specifically designed for security issues in an e-commerce environment, and the increased use of encryption technology.
- Eighty-eight percent of respondents feel that the public perceives the traditional, or established "bricks and mortar" business as being more secure than e-commerce based dot.com companies.

Overall, we did not identify many significant disparities among the reporting regions. National and geographic boundaries are non-existent in the growing world of e-commerce – e.fr@ud and security related risks affect all businesses.



About our Research

Many experts believe that fraud-related crimes have been greatly assisted by the introduction of the Internet and e-commerce and that the perpetration of e.fr@ud is on the rise. No country or company is immune to the depredations of the fraudster. In view of the explosive growth of e-commerce in the global market, the third international KPMG Fraud Survey is focused entirely on e.fr@ud and security related issues in the world of e-commerce.

In 2000, KPMG Forensic & Litigation Services practices sent questionnaires on e-commerce and e.fr@ud to more than 14,000 CEOs, CIOs, and other senior executives of the largest public and private companies in the following 12 participating countries:

Australia	India
Belgium	Italy
Canada	South Africa
Denmark	Switzerland
Germany	United Kingdom
Hong Kong	United States

This report presents the main findings of the national surveys and compares the findings of individual countries in order to provide insight into e.fr@ud and security on an international basis.

Where appropriate, we have grouped countries by geographic region, summarized as follows:

Region	Countries
Asia Pacific	Australia, Hong Kong, India
Europe, Middle East and Africa (EMEA)	Belgium, Denmark, Germany, Italy, South Africa, Switzerland, United Kingdom
Americas	Canada, United States

The purpose of this global survey was to establish the degree to which the world's largest companies have engaged in e-commerce activities, to determine how internal and external attacks on e-business infrastructure are impacting different companies, and to determine how these companies are responding to the threat of such security breaches.

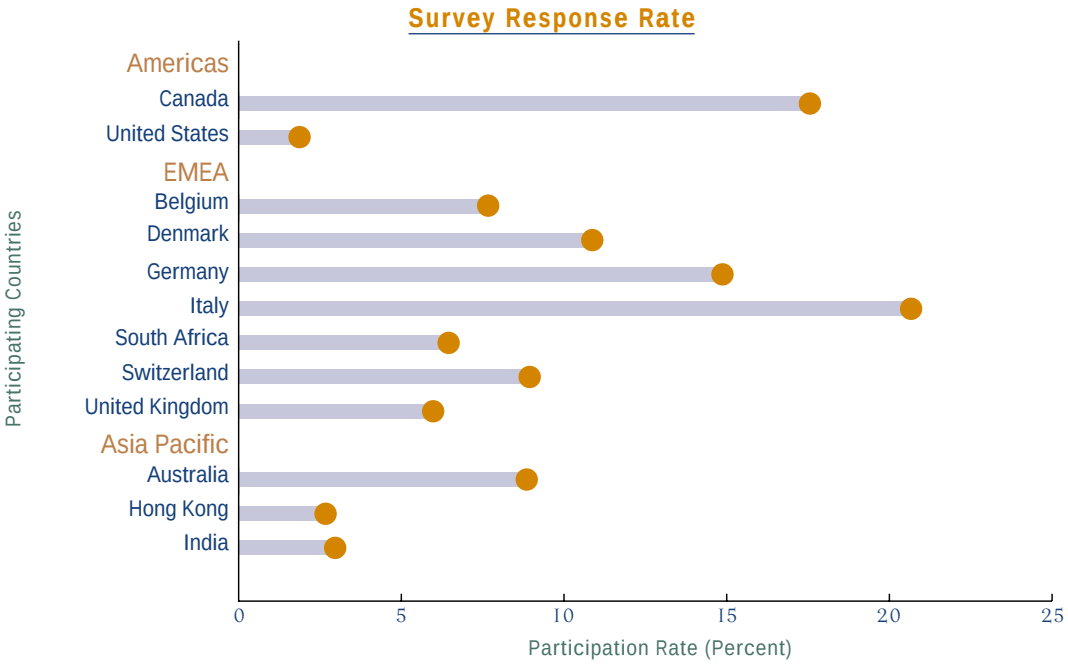
Specifically, we asked survey respondents questions that explored the following issues[1]:

- Their level of awareness of e.fr@ud and security-related risks associated with e-commerce;
- The extent to which their company is at risk of e.fr@ud and security-related breaches;
- The nature and extent of preventative measures implemented by their company to minimize e.fr@ud and security-related risks in e-commerce; and
- Their impression of their customers' perceptions about e-commerce security.

[1] The survey responses reflect the experience and insights of the individual respondents.

While there was a large variation in response rates among the participating countries, an average response rate of 9 percent was achieved. The rate of response to this year's survey is lower than our more traditional Fraud Surveys. Not all participants have embraced e-commerce, with the result that they may have chosen not to respond to the survey.

In total, 1,253 completed questionnaires were included in the survey findings[2]. A summary of the survey participation rates, broken down by participating country, is provided below:



The following table summarizes the total number of responses that were received from each participating country:

Country	Number of Respondents	
Canada	179	
United States	65	
Americas		**244**
Belgium	80	
Denmark	68	
Germany	152	
Italy	315	
South Africa	102	
Switzerland	93	
United Kingdom	50	
EMEA		**860**
Australia	92	
Hong Kong	24	
India	33	
Asia Pacific		**149**
Total Number of Respondents		**1,253**

[2] Response rates varied from question to question. That is, not all 1,253 participants responded to all questions asked.

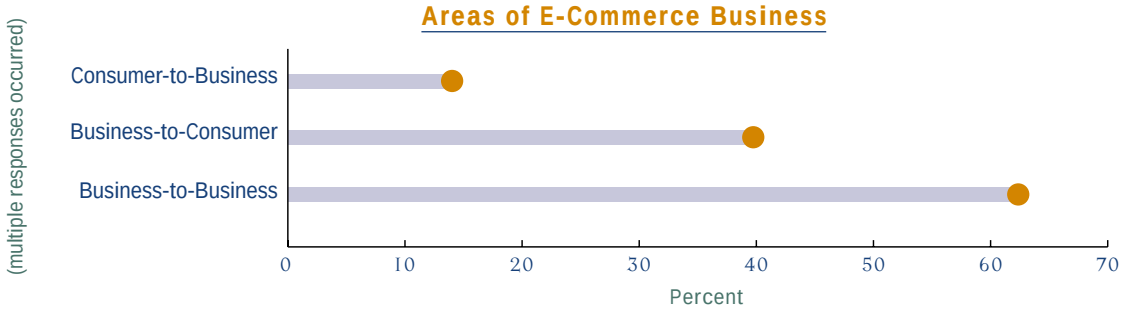
E-COMMERCE IN THE WORLD'S LARGEST COMPANIES

While there are various definitions of e-commerce, it can generally be described as a system that conducts business communications and transactions electronically – the buying and selling of goods and services, and the transfer of funds, through digital communications. The main vehicles for e-commerce continue to be the Internet and the World Wide Web. However, electronic mail (e-mail), facsimile, and telephone orders are commonly used for e-commerce transactions. Typically, there are three types of e-commerce transactions: business-to-business, business-to-consumer, and consumer-to-business.

We asked survey participants how knowledgeable they consider themselves to be with respect to e-commerce within their organization. Eighty-six percent of respondents considered themselves somewhat to very knowledgeable about e-commerce. However, approximately 20 percent of survey respondents from Belgium, Germany, Italy, and Hong Kong reported that they were not very knowledgeable about e-commerce within their respective organizations.

Survey participants were asked whether their companies are engaged in e-commerce transactions. Sixty-two percent of respondents said that their company had engaged in some form of e-commerce. Of the companies that are engaged in e-commerce, 63 percent are involved on a "business-to-business" basis, while 41 percent are engaged in transactions directly with consumers ("business-to-consumer")[3]. Several respondents stated that their companies were in the process of establishing an e-commerce system. This demonstrates the increasing importance of e-commerce to businesses.

Only 21 percent of respondents indicated that their e-commerce activities were limited to web-page exposure. Although not engaged in e-commerce transactions, these companies can be just as affected by e-commerce security-related issues as those who are – the defacement of a web page can have a long-lasting, detrimental impact on a company's reputation for security, or the lack thereof.



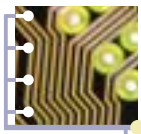
[3] Multiple responses occurred.

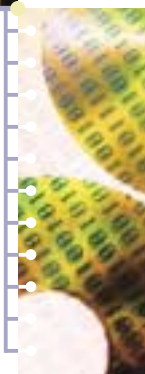
Eighty-eight percent of respondents reported that their e-commerce activities accounted for less than 10 percent of their company's total revenue. Several respondents from the United States and other countries commented that the implementation of a full e-commerce system has been prevented by a lack of demand in the marketplace. This comment is consistent with the reported level of revenue generated from e-commerce activities.

However, we would expect the percentage of revenue generated from e-commerce activities to grow significantly as companies embrace the emerging digital economy and implement more sophisticated e-commerce security measures.

Survey participants were asked what prevented, or is preventing, them from implementing a full e-commerce system at their company. Fifty percent of respondents identified cost as a major inhibitor to implementing a full e-commerce system. The availability of skills and security of information and privacy issues were also rated by respondents as major inhibitors to the implementation of a full e-commerce system. The following table summarizes the respondents' ratings of the issues identified (note: multiple responses occurred):

Factors that Prevented or are Preventing the Implementation of Full E-Commerce System

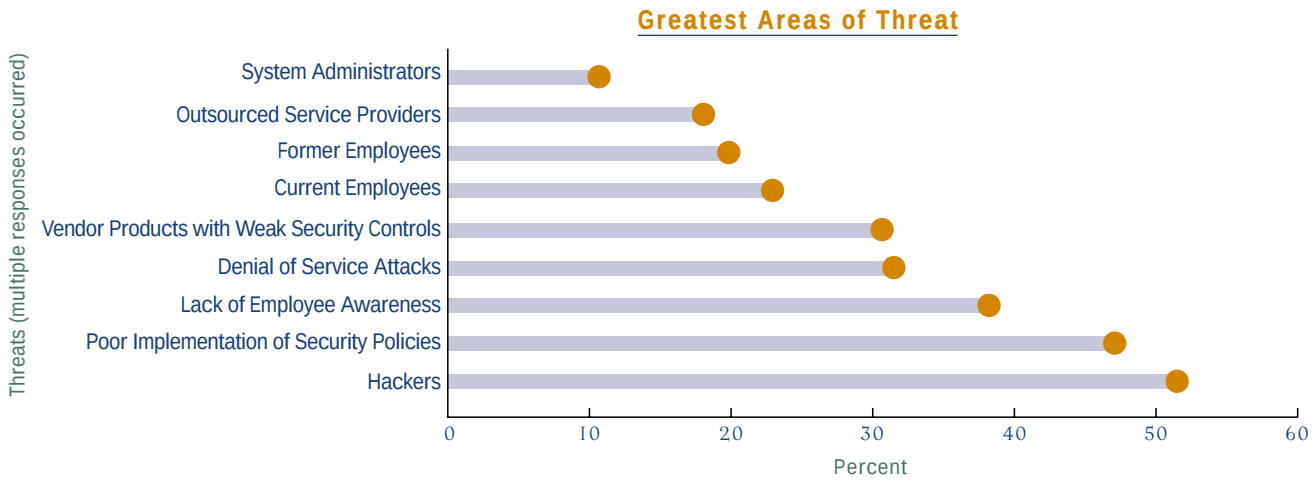




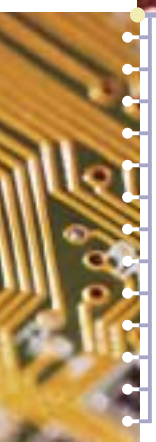
AWARENESS OF E.FR@UD AND E-COMMERCE SECURITY RISKS AND THREATS

One of the biggest issues organizations must take into account when utilizing e-business initiatives is security. E-commerce systems are continuously exposed to internal and external threats. Survey participants were asked what they considered the greatest threats to their company's e-commerce system.

Hackers, poor implementation of security policies, and the lack of employee awareness were identified by survey participants as the greatest areas of threat to their e-commerce systems. The survey responses were consistent for all participating countries – each country identified as their greatest threats a minimum of two of the three threats identified above[4].



Security breaches through Internet connections are typically attributed to hackers. These breaches are often classified by the affected companies as breaches caused by "external" perpetrators. However, based on our experience, most security breaches perpetrated through Internet connections are committed by individuals who possess intimate knowledge of the systems that they are attacking. Disgruntled or former employees may commit the breach themselves, or they may supply the information necessary to commit the breach to a more knowledgeable person, who will commit the breach on their behalf.



[4] This information was not requested in the Canadian survey.

- Respondents felt that the greatest potential threats to the success of their e-commerce efforts were security for online systems, system availability (i.e., risk of denial of service attacks), confidentiality of customer and company information, and the maintenance of the integrity of this data.
- Seventy-nine percent of survey respondents indicated that a security breach to their e-commerce system would most likely result from a breach caused via the Internet or other external access. Respondents were more confident in the other components of their e-commerce systems, including internal systems, physical security, and responses to system failure. Seventy-two percent of respondents from India rated the threat of a security breach over their internal systems as high. Most respondents considered the risk of a breach occurring as a result of human error (such as system security patches not being implemented) to be moderate.
- Respondents have a great deal of confidence in the various components of their e-commerce systems, including:
    - Backup systems;
    - Internet connection;
    - Connections to internal systems and staff;
    - Electronic transactions storage; and
    - Connections to suppliers, banks, shippers, etc.
- We asked respondents to rate the likelihood of damage that could be caused to the various components of their e-commerce systems as a result of a security breach. Seventy-two percent of respondents reported that their greatest area of concern was with respect to the risk of any damage that could be detrimental to their company's reputation. We believe that a company's desire to protect its reputation is primarily responsible for many frauds going unreported – many companies prefer to deal with the discovery of fraud as an internal matter, away from public scrutiny. The threat of damage to the other components of their e-commerce systems was rated low to moderate.
- Respondents cited weak internal controls or barriers, malice without economic gain, and grievance on the part of an employee as the three factors most likely to result in their e-commerce system being the target of a security breach.
- Eighty-three percent of survey respondents believe that their e-commerce system is more of a target for fraud than their non e-commerce systems. The most commonly rated reason was the greater market exposure associated with e-commerce. An Australian respondent identified the high monetary value of transactions involved with the Financial Services industry as being a particularly risky area. Other respondents commented on the greater risk resulting from the perpetrators' perceived ability to maintain anonymity in an e-commerce environment.

E.FR@UD AND SECURITY BREACHES

Seventy-eight percent of the individuals who completed the survey questionnaires believe that they would be made aware of an e-commerce system security breach that occurred in their company in a timely manner.

Survey participants were then asked if they were aware of any security breaches involving the e-commerce systems in their company. Sixty-two percent of our survey participants responded to this question. Only 9 percent of respondents indicated that a security breach had occurred within the last 12 month period. Respondents from India reported the highest rate of e-commerce security breaches at 23 percent, followed by approximately 14 percent of respondents from Germany and the United Kingdom.

Based on recent media reports, we believe that the number of reported breaches by respondents is understated. There may be a variety of explanations for this understatement, including:

- An understandable reluctance to report such information;
- Respondents not having been made aware of security breaches that had occurred within their organization;
- Many attacks or intrusions going undetected by the organization; or
- Survey participants sustaining a security breach may have chosen not to respond to this question.

For the purposes of our survey, we have identified internal breaches as those perpetrated by individuals within the organization, including those caused by perpetrators with an established relationship with the company (i.e., former employees and external service providers). Breaches perpetrated by individuals unknown to the organization would be considered external.

Respondents indicated that where a security breach had occurred, it was approximately three times more likely to be caused by external intruders than internal intruders. The damage caused, or attempted to be caused, by the reported security breaches were primarily viruses being planted on the system, system crashes, web site defacement or alteration, and/or system resources being redirected or misappropriated.

Survey respondents were able to determine the identity of the perpetrator in approximately one-half of the breaches that were reported over the last 12 month period. We find this rate to be surprisingly high. The reconstruction of an electronic trail left by a perpetrator can be very difficult to achieve. This task is more complex if an external party has perpetrated the breach. As the Internet has no boundaries, the investigation needs to consider a variety of laws and privacy regulations in various

jurisdictions when tracking the electronic trail to identify the perpetrator of the breach. For example, an investigator will require legal approval in most instances to obtain a source's user information. This cumbersome process may dissuade companies from pursuing an investigation.

It is possible that respondents have included former employees or external service providers in their classification of "external" breaches. In reality, these perpetrators have a strong "internal" relationship established with the organization.

Approximately 83 percent of respondents stated that legal action was not pursued when a breach occurred. Various explanations were provided, including:

- Inadequate legal remedies available;
- Obtaining an out-of-court settlement;
- Loss sustained as a result of the breach was not quantifiable;
- No possibility of recovery;
- Lack of evidence; and
- Other explanations.

One respondent from Denmark stated that legal action was not pursued as the perpetrator showed the security gap to the company's Information Technology group. A respondent from the United Kingdom made a similar comment – the perpetrator notified the company of the potential to deface its web site, but no damage was actually committed. The respondent noted that the perpetrator was helpful and not considered malicious. Other respondents stated that legal action was not pursued, as damage was not sustained as a result of the security breach. Many companies will not be so fortunate.

E-commerce is a relatively new and rapidly growing business medium. Companies have only just begun to experience e.fr@ud and security breaches. Recent media reports of some relatively high-profile denial-of-service attacks or the release of Trojan viruses are just the beginning. Many more organizations have likely been the target of e.fr@ud but have been reluctant to go public with this information.

When a security breach has been detected, a company's initial response is typically to resolve the problem right away and bring their e-system back up for business. E-system down-time is synonymous with lost revenue. However, the main concern should be to identify the source of the breach and determine whether it is an internal or external problem. This information will affect the scope and focus of the investigation.

The immediate resolution of the problem by the internal system administrators and/or Information Technology (IT) personnel will often compromise the integrity of the data, thus causing the evidence of the breach to be corrupted. As a result, the likelihood of the company to be in a position to attempt to recover assets and/or pursue legal action will be more difficult or impossible.

These problems can be avoided with the existence and use of proper incident response procedures. The initial steps should include a close working relationship with trained computer forensic professionals. The evidence-gathering procedures followed, and the integrity of the data obtained, may come under scrutiny if litigation ensues. Accordingly, any investigation should include the proper recovery and preservation of the original data. Properly recovered data may produce evidence that will form the foundation for further in-depth investigations, the recovery of misappropriated assets and/or the use in potential litigation.

PREVENTION AND DETECTION OF E.FR@UD AND SECURITY BREACHES

Many companies are complacent when it comes to issues related to e.fr@ud and security breaches. The reality is that all companies that have embraced e-commerce will be exposed to e-fr@ud.

Our survey asked respondents about measures their companies had taken with respect to the prevention and detection of e.fr@ud and security breaches. It is apparent that, while basic preventative measures may have been taken, e-commerce security still requires significant improvement, as demonstrated by the following:

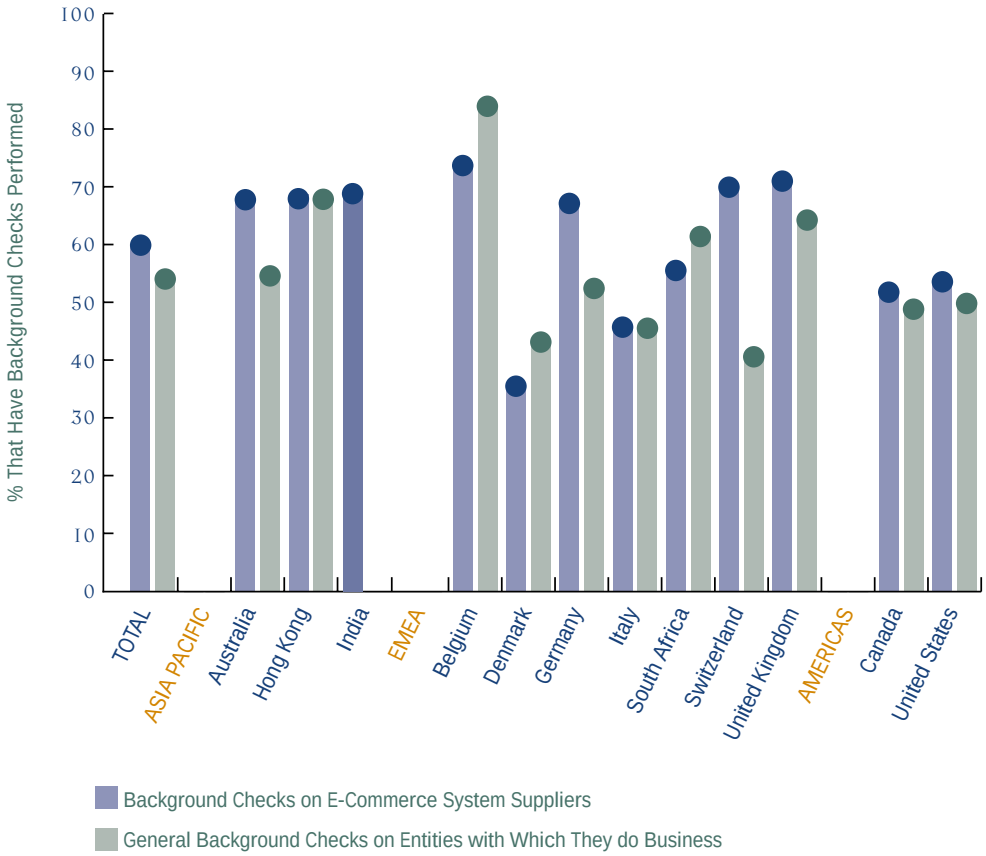
- Thirty percent of survey respondents, including those who had only one system administrator, do not have adequate segregation of duties with respect to the maintenance of their e-commerce system.
- Sixty-six percent of respondents do not have security audits performed on their e-commerce systems.
- Sixty-two percent of respondents stated that background checks were performed on the entities that assist them with the development, maintenance, and/or administration of their e-commerce system. Denmark and Italy reported significantly lower usages of background checks at 37 and 48 percent, respectively.

  Fifty-six percent of respondents stated that background checks were generally performed on entities with which they do business. Belgium reported the highest rate of usage of background checks at 86 percent. In contrast, Denmark, Italy, and Switzerland were significantly lower, averaging approximately 45 percent[5].

  Every day we put our trust in employees and business partners. But are they worthy of our trust? Many organizations fail to perform appropriate background checks on the people they hire or do business with.

[5] The India survey did not ask the question regarding the general use of background checks.

Background Checks

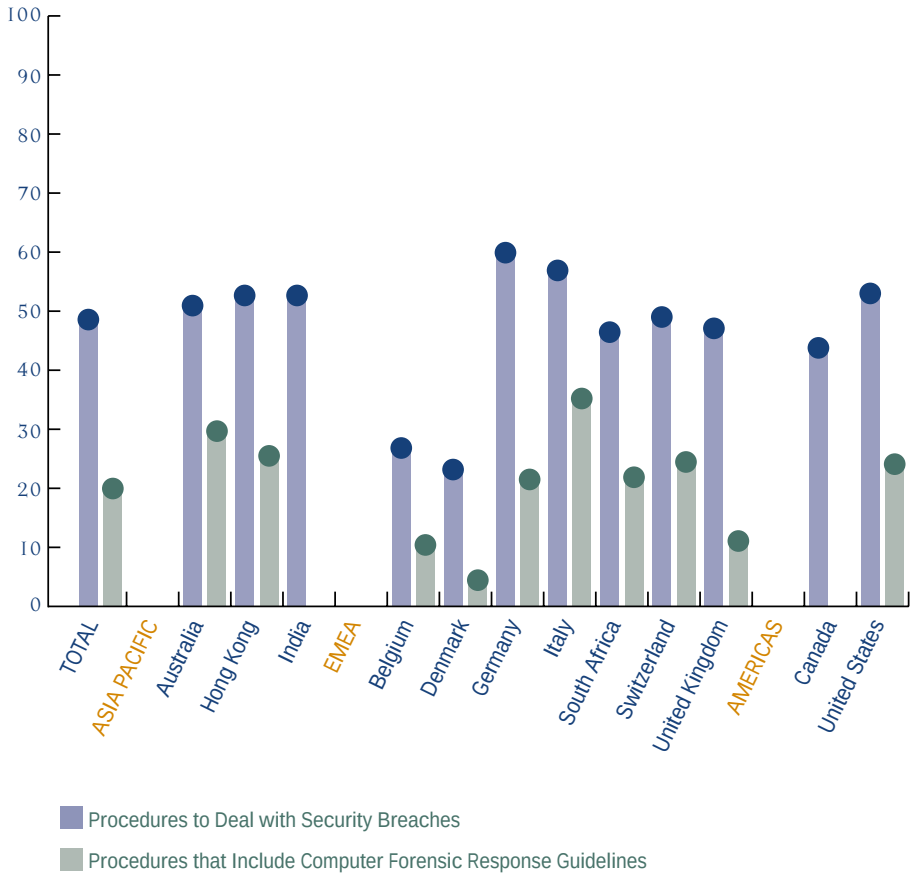


The nature and extent of the background check performed will vary significantly depending on the nature of the assignment. The IT personnel maintaining an e-commerce system have a tremendous amount of control and influence over electronic assets. The level of background checks performed should be commensurate with the level of risk associated with the position. Such background checks may range from pre-employment screening, including criminal record checks and consultation with former employers, to due diligence, which may include the verification of certificates and credentials represented by the applicants.

- One-half of respondents stated that their organization has incident response procedures to deal with security breaches of their e-commerce system. Germany and Italy reported the highest usage rates, averaging 60 percent, while Belgium and Denmark reported the lowest usage rates, averaging only 27 percent.

  Of those respondents who have incident response procedures, only 43 percent (or 22 percent of total respondents) have procedures that include computer forensic response guidelines to deal with wilful intrusions into their networks and to ensure proper evidence gathering. Australia and Italy reported the highest rate of respondents who included computer forensic response guidelines in their incident response procedures at 60 and 63 percent (31 percent and 37 percent of total respondents), respectively. Denmark and the United Kingdom reported the lowest rate of respondents whose incident response procedures included computer forensic response guidelines at 25 percent (6 percent and 13 percent of total respondents, respectively)[6].

Incident Response Procedures



[6] The surveys in India and Canada did not ask the question regarding the existence of computer forensic response guidelines.

- Only 12 percent of respondents stated that their web site bears a seal identifying that their system has passed a security audit. Although the majority of the respondents from the participating countries had similar usage rates, only 2 percent of respondents from Australia and the United Kingdom reported that their web site bears a security audit seal. In contrast, South Africa reported the highest usage rate at 20 percent.

  Overall, the usage of web site security audit seals is low. This may indicate that web site security audits are not currently regarded as an effective security precaution, or that this form of security is not well known or understood.

Survey respondents from all participating countries stated that security of their e-commerce system could be most improved by the following:

- Regular system penetration testing (authorized hacking);
- Use of software specifically designed for security issues in an e-commerce environment; and
- Increased use of encryption technology.

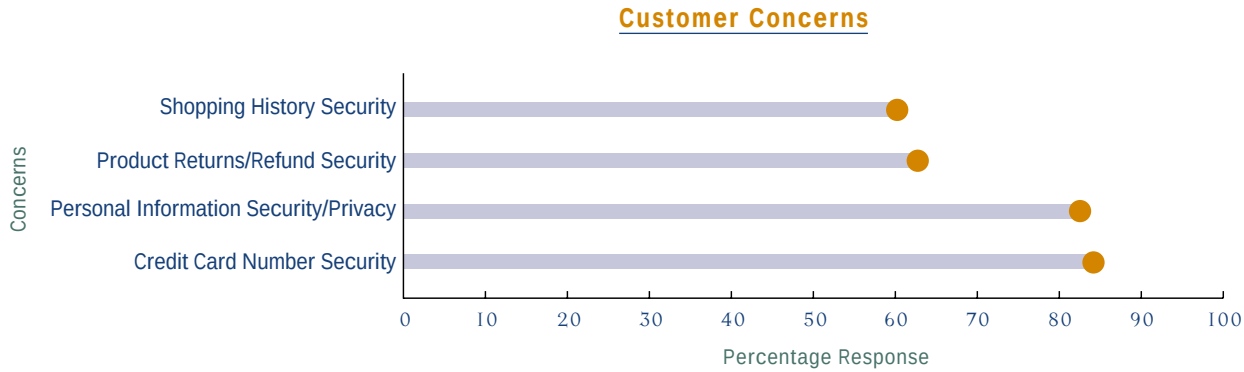
The performance of regular third-party audits and upgrading software currently in use were elements that were considered by survey respondents to moderately improve the security of their e-commerce systems. Additional staff, increased legal remedies, and government intervention were identified by survey respondents as the elements least likely to improve the security of their e-commerce systems.

Our experience shows that, in many cases, internal breaches have involved an IT professional, either wittingly or unwittingly. Security breaches may be caused by errors made within a company's IT department (e.g., when a system administrator erroneously leaves a portion of a company database unprotected during a system upgrade). Alternatively, disgruntled IT staff may be the culprits committing the irregular activities.

A comprehensive security program will assist in the prevention and detection of e.fr@ud and security breaches from all sources. The use of various layers of properly implemented protection mechanisms will have the synergistic affect of increasing and enhancing a security program. Encryption, firewalls, intrusion detection systems, incident response procedures, monitoring and audits performed by external specialists are examples of items used to increase or enhance the security of an e-commerce system. No one component alone is sufficient to protect electronic assets. This "onion" model of security is currently considered by many experts to be the best and safest approach to managing the risks associated with e-business.

CONSUMER PERCEPTIONS ABOUT E-COMMERCE SECURITY

Survey participants were asked what issues are of most concern to their customers with respect to e-commerce transactions. Respondents indicated overwhelmingly that security of credit card numbers and personal information were by far the most important concerns to their customers. Security of information relating to personal shopping history and the organization's return and refund security policies were considered to be low to moderate areas of concern.



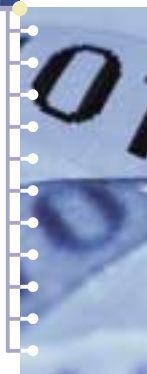
Survey participants were also asked for their views on public perceptions about e-commerce security:

- Eighty-eight percent of respondents feel that the public perceives the traditional, more established "bricks and mortar" businesses as being more secure than e-commerce based, or dot.com, companies.
- Respondents identified concerns about the security and privacy of information and a lack of familiarity with technology as being the most important factors preventing the public from engaging in e-commerce transactions. A respondent from the United Kingdom also indicated that customers are hesitant to engage in e-commerce due to the lack of personal interaction – the lack of "physical" contact with the company selling the goods or services.
- Delivery concerns, lack of Internet access, and Internet/computer speeds were not considered significant deterrents to the public's use of e-commerce.

SURVEY PARTICIPANTS

Survey participants represented a cross-section of industries. The areas of businesses around the world represented by the responses were as follows[7]:

Industry Sector	Percent of Respondents
Agribusiness	3
Automotive and Industrial Products	14
Business Services	4
Chemicals and Pharmaceuticals	5
Consumer Markets (Food, Drink, and Consumer Products)	12
Electronics/Technology	7
Energy and Natural Resources	9
Financial Services and Insurance	15
Government and Educational Institutions	4
Publishing/Printing	3
Real Estate, Building, and Construction	5
Transportation	4
Wholesale Distribution	11
Other	4
	100 %



[7] 1,054 out of 1,253 survey participants provided a response. Ninety-three survey participants provided a response that included more than one Industry Sector.

About KPMG

KPMG is the global network of professional service firms whose aim is to turn understanding of information, industries and business trends into value. With more than 100,000 people worldwide, KPMG member firms provide assurance, tax and legal, financial advisory and consulting services from more than 800 cities in 155 countries. KPMG's Web site is: www.kpmg.com

KPMG's Forensic & Litigation Services practice provides a broad range of global services to clients of all sizes in both the public and private sectors. Our in-depth experience ranges from conducting complex financial and non-financial investigations to the implementation and monitoring of vendor monitoring programs for organizations around the world. We also provide fraud risk management, corporate intelligence, litigation support, dispute resolution, intellectual property, and anti-money laundering services.

Our team of professionals include: Investigative Accountants, Former Law Enforcement Officers, Private Investigators, Business Valuators, Criminologists, Computer Forensic specialists and Engineers.

For more information on KPMG's Forensic & Litigation Services, please contact one of the following individuals:

Country	Contact	Telephone	Facsimile	E-mail
Australia	David Van Homrigh	617 3233 3205	617 3220 0107	djvanhomrigh@kpmg.com.au
Belgium	Evert-Jan Lammers	32 2 708 3912	32 2 708 39 11	ejlammers@kpmg.com
Canada	Norman Inkster	416 777 3255	416 777 3519	ninkster@kpmg.ca
Denmark	Jesper Koefoed	45 38 18 35 36	45 38 18 30 45	jkoefoed@kpmg.com
Germany	Dieter John	49 221 2073 1575	49 221 2073 411	de-integrityservices@kpmg.com
Hong Kong	Mike Watson	852 2826 80 38	852 2973 66 16	mike.watson@kpmg.com.hk
India	Deepankar Sanwalka	91 11 341 1222	91 11 341 3880	dsanwalka@in.kpmg.com
Italy	Stefano Fortunato	3902 6763 2637	3902 6763 2638	sfortunato@kpmg.it
South Africa	Petrus Marais	27 21 423 8940	27 21 423 8937	petrus.marais@kpmg.co.za
Switzerland	Peter Cosandey	41 1 249 2231	41 1 249 2233	pcosandey@kpmg.com
United Kingdom	Alex Plavsic	44 20 7311 3862	44 20 7311 3630	alex.plavsic@kpmg.co.uk
United States	Tom Talleur	202 533 6046	202 533 8549	ttalleur@kpmg.com

> “National and geographic boundaries are non-existent in the growing world of e-commerce – e.fr@ud and security related risks affect all businesses.”

Printed in Canada on recycled paper. 2126.01.03E