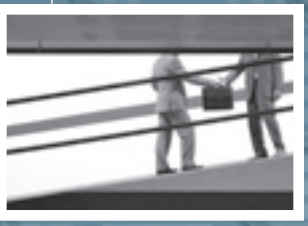
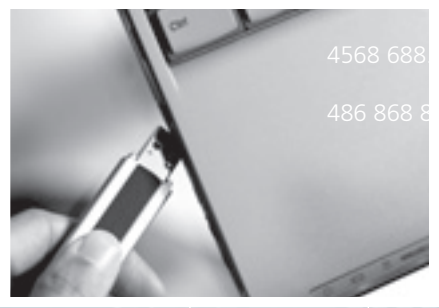
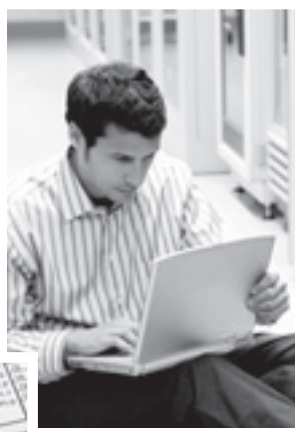
McAfee

Unsecured Economies: Protecting Vital Information

The first global study highlighting the vulnerability of the world's intellectual property and sensitive information.







CONTENTS

1 **Foreword**

2 **Introduction**

4 **Key Finding 1:** Valuable Data is Being Moved—and Lost

8 **Key Finding 2:** The Current Economic Downturn May Be a Perfect Storm for Security Breaches

12 **Key Finding 3:** Geopolitical Perceptions Have Become a Reality in Information Security Policies

18 **Key Finding 4:** Intellectual Property is a New Currency for Cybercriminals

22 **Future Challenges and Recommendations**

28 **Conclusion**

30 **Contributors**

Contributors

Nick Akerman
Dr. Ross Anderson, Ph.D.
Dr. Ashish Arora, Ph.D.
Augusto Paes de Barros
Renato Opice Blum
Lynn Robert Carter
Lilian Edwards
Gail F. Farnsely
Dr. Marco Gercke
Karthik Kannan
Sivarama Krishnan
Heejo Lee
Tom Longstaff, Ph.D.
Jacquelyn Rees
Dr. Timothy J. Shimeall, Ph.D.
Eugene H. Spafford
Professor Yoshiyasu Takefuji, Ph.D.
Professor Katsuya Uchida, Ph.D.
Michael Versace
Dr. Sun Yuqing, Ph.D.

Foreword

As we face one of the worst recessions in recent memory, protecting a company's critical information assets like intellectual property and sensitive data has never been more important, yet challenging. A single breach or loss can cause irreparable financial damage to a company's reputation, its share price and customer confidence. It's a risk companies can't afford in the current climate.

How vulnerable are companies to losing the intellectual property and sensitive data that makes them successful? Which countries are emerging as clear sources of threats to the world's vital information? And how has the economy led to new threats?

McAfee decided to take a hard look at these questions and consulted with global senior IT decision makers from 1,000 large organizations and dozens of security and business experts from top institutes. The findings were startling. It's not something we take lightly at McAfee.

Companies surveyed estimated that they lost an average of $4.6 million worth of intellectual property in 2008. Forty-two percent said laid-off employees were the single biggest threat to their intellectual property and other sensitive data they faced in the current economic climate.

Intellectual property and sensitive data has become a premium currency for financially desperate or laid-off employees. Cybercriminals also see this vital information as a high value commodity and are devising increasingly devious ways to infiltrate companies through its employees. And finally, China, Russia and Pakistan are emerging as clear sources of threats to vital corporate data.

At McAfee we are committed to helping companies and governments safeguard their vital information. We know technology alone isn't the answer. As part of McAfee's initiative to fight cybercrime, we recently established a global cybercrime council of business leaders and CIOs to tell us what we need to do to better protect their organizations from these multiple threats.

For me this report is a timely wake-up call that businesses need to shift their mindsets in the way they value intellectual property and other sensitive information.

Dave DeWalt
President & CEO
McAfee, Inc.

Introduction

Businesses around the world are being squeezed by the economic downturn, and the uncertainty facing them is compounded by significant risks due to data leakage, data loss and outside attacks, all of which have increased significantly over the past year.

How is the current economic downturn impacting the ability of organizations to protect vital information such as intellectual property? Which countries pose the biggest threat to economic stability in others? How are cybercriminals targeting enterprises across all geographies? How will the protection of digital assets help or hinder a global economic recovery in the coming year?

In collaboration with experts in the fields of data protection and intellectual property, McAfee took a hard look at these questions. Commissioned by McAfee, Professors Karthik Kannan, Jacquelyn Rees and Eugene H. Spafford from Purdue University and the Center for Education and Research in Information Assurance and Security (CERIAS) undertook extensive research with experts from around the globe. International research firm Vanson Bourne surveyed more than 1,000 senior IT decision makers in the U.S., U.K., Japan, China, India, Brazil and the Middle East to develop the most in-depth study on this topic to date.

The result is *"Unsecured Economies, Protecting Vital Information,"* which reveals the extent to which the economic downturn is set to impact the security of vital information as CIOs attempt to secure critical information across continents and companies. Information is becoming firmly established as an international form of currency, and cybercriminals are increasingly targeting businesses for profit. The sources of threats are shifting, and new nations are emerging as perceived threats to data security.

The report concludes with suggested best practices for protecting valuable digital assets, not only in order to survive—but to thrive—in these challenging times.

Four Key Findings Emerge

1: The research indicates that more and more vital digital information, such as intellectual property and sensitive customer data, is being transferred between companies and continents—and lost. The average company has $12 million (USD) worth of sensitive information residing abroad. Companies lost on average $4.6 million worth of intellectual property in 2008.

2: The global economic crisis is poised to create a perfect information security risk storm, as increased pressures on firms to reduce spending and cut staffing lead to more porous defenses and increased opportunities for cybercriminals. Forty-two percent of respondents interviewed said laid-off employees are the biggest threat caused by the economic downturn.

3: Elements in certain countries are emerging as clear sources of threats to sensitive data, in particular to intellectual property. Geopolitical perceptions are influencing data policy reality, as China, Pakistan, and Russia were identified as trouble zones for various legal, cultural and economic reasons.

4: Cyberthieves have moved beyond basic hacking and stealing of credit card data and personal credentials. An emerging target is intellectual property. Why sink all that time and money into research and development when you can just steal it?

KEY FINDING 1:
Valuable Data is Being Moved—and Lost

The research indicates that more and more vital digital information, such as intellectual property and sensitive customer data, is being transferred between companies and continents. It also indicates that much of it is being lost in the process.

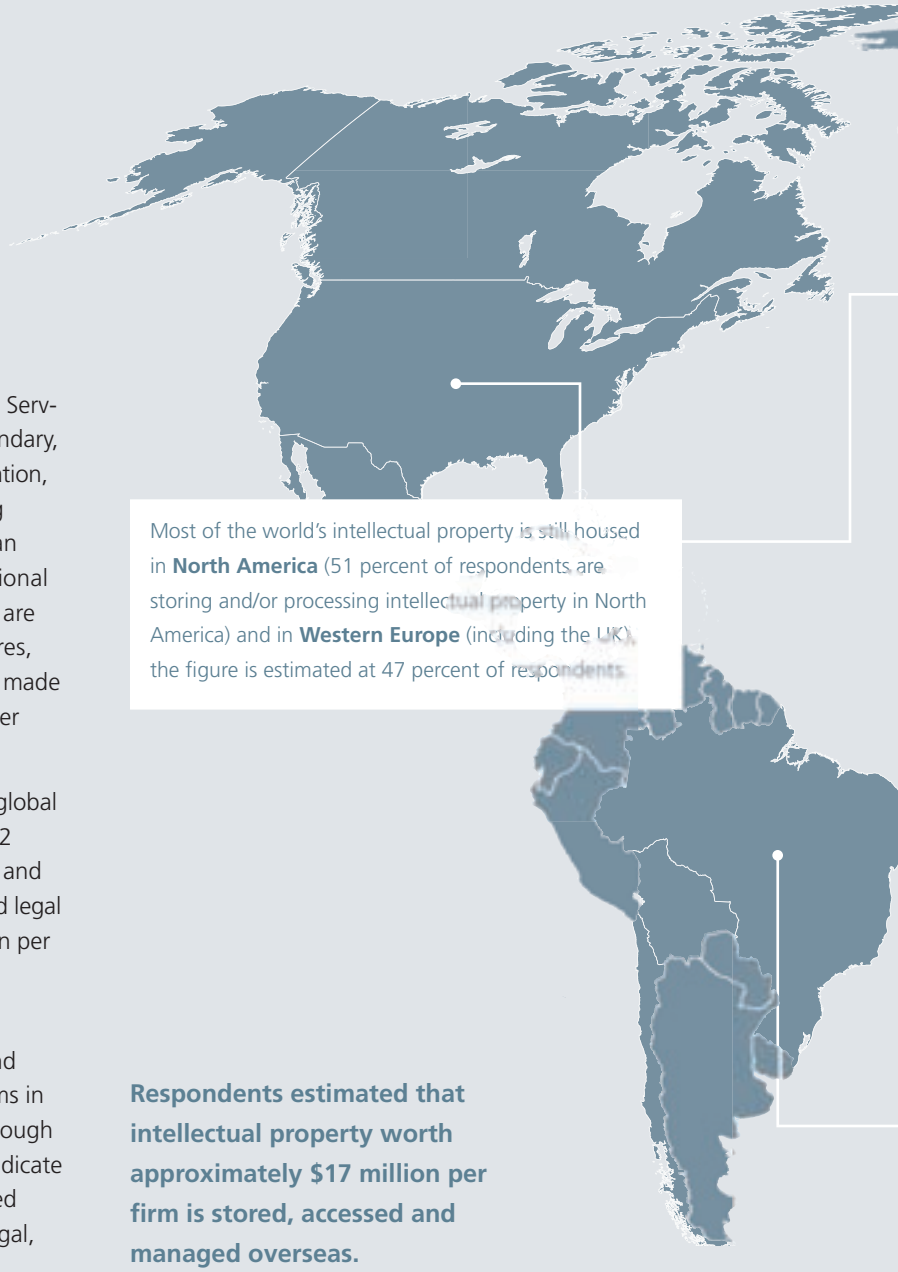
The Growing Corporate Risk to Intellectual Property

The dispersion of vital information offshore: The average company has $12 million worth of sensitive information residing abroad

According to Michael Versace, senior advisor at Financial Services Technology Consortium (FSTC), the operational boundary, which he refers to as the "trust boundary" of an organization, has considerably expanded. With many companies having subsidiaries and satellite offices around the globe and an increased need for collaboration, the traditional operational boundaries are now disappearing. Informational assets are subject to various jurisdictions, infrastructure and cultures, including those of suppliers and partners. This trend has made it more difficult to lock down intellectual property in order to ensure its safety.

The research validates this claim. Respondents from the global companies interviewed estimated that on an average $12 million worth of sensitive information, such as customer and credit card data, intellectual property, financial records and legal documents, resides overseas. This ranges from $8.2 million per Japanese firm to a high of $15.2 million per U.K. firm.

Respondents estimated that intellectual property worth approximately $17 million per firm is stored, accessed and managed overseas. This ranges from $1.4 million for firms in Brazil to $61 million for firms in China. While these are rough estimates and are likely to be on the low side, they do indicate that a substantial amount of intellectual property is stored outside the home country and might be at risk due to legal, cultural and political differences.



Most of the world's intellectual property is still housed in **North America** (51 percent of respondents are storing and/or processing intellectual property in North America) and in **Western Europe** (including the UK), the figure is estimated at 47 percent of respondents.

Respondents estimated that intellectual property worth approximately $17 million per firm is stored, accessed and managed overseas.

Estimates on the total value of global intellectual property stored "offshore" from home countries are hard to find. However, out of more than 500 firms in our sample, 197 reported a combined $3.4 billion of intellectual property stored overseas.

Eastern European countries with strong technical backgrounds, such as Romania, have also been gaining considerable attention in their ability to serve Western European countries. Approximately 40 percent of German companies, for example, have their data served by **Eastern European countries.**

China's manufacturing industries and the government's mandatory inspection of the manufacturing equipment of foreign firms has also increased the concentration of intellectual property there, despite concerns of rampant reverse engineering of devices. Thirty-six percent of respondents are storing or processing data in Eastern Asia, a region including **China, Japan and South Korea.**

There has been an increase in outsourcing activities in **India, the Philippines, Brazil** and other countries which have effectively diminished the concentration of intellectual property in some areas. Twenty-two percent of respondents are storing and/or processing intellectual property in **South-Central Asia** (including India and Pakistan), and 19 percent are storing and/or processing intellectual property in **South or Central America.**

Why companies are moving vital information offshore

A number of factors are influencing the trend for companies to store vital information offshore. Twenty six percent of respondents cited cost reduction, as labor is often substantially less expensive in many overseas locations than in the U.S. and Canada, Western Europe, Japan and Australia. Other drivers for storing or processing sensitive information outside of the home country were supply chain partner efficiency (33 percent) followed by better expertise (30 percent) and increased safety (29 percent).

The ability to safely store vital information is a key factor according to respondents in several countries, including Brazil, Japan and, most notably, China. In fact, more than 60 percent of Chinese respondents cited "safer storage available elsewhere" as a reason for storing or processing sensitive data outside of the home country.

Commitment to protecting vital information varies

Considering how much vital information companies are moving offshore, in the current economic climate it is more important than ever that this data is secure. The research findings suggest this may not necessarily be the case.

The research indicates that companies in developing countries are more motivated and spend more on protecting vital information than their Western colleagues.

Respondents in countries such as Brazil, China and India spent more on security as a percentage of their overall IT budgets, while respondents in developed countries such as Germany, Japan, the U.S. and the U.K. said they proportionally spent less on protecting their vital information. Thirty five percent of Indian, 33 percent of Chinese and 27 percent of Brazilian firms reported spending 20 percent or more of the IT budgets on security, compared to 20 percent of German, 19 percent of U.S., 10 percent of Japanese, and four percent of U.K. firms. The U.K. reported the least amount of spend on security as a percentage of their IT budget, with 44 percent of the U.K. respondents spending zero to five percent of their IT budgets on security.

When comparing the motivators of information security investments, there is a striking difference in attitude. It appears that decision makers in many countries, particularly developed ones, are reactive rather than proactive. Compliance with regulation is the key motivator in Dubai, Germany, Japan, the U.K., and the U.S. Seventy-four percent of Chinese respondents and 68 percent of Indian respondents, however, reported making decisions based on gaining and/or maintaining a competitive advantage in attracting customers or clients.

While societal protection (enforcement and other actions) of information assets is weaker in India and China than in developed countries, the company-level organizational commitment in these countries is not. For example, a manager in an Indian IT outsourcing company mentioned, even before the recent Mumbai attacks, that his company had well-defined business continuity plans and has drills once every six months, sometimes even pretending a terrorist attack took out one of its sites.

Pursuing intellectual property security incidents varies

To make matters worse, there are a minority of companies in some countries who did not pursue a security incident. This suggests that when intellectual property is stolen in certain countries, it will not be reported.

Among Chinese firms, 28 percent said they do not pursue security incidents because of the cost, and 35 percent do not pursue them to avoid bad publicity. Twenty-three percent of German and Japanese firms and 19 percent of Indian firms said they don't respond to incidents because of the cost.

Interestingly, 24 percent and 22 percent, respectively, of Dubai and Indian firms did not investigate security incidents because of a lack of "cooperation." This resistance could exist at the firm, local, federal, or international level but indicates that neither all firms nor all agencies are fully cooperative in addressing these problems.

Companies to cut spending on protecting intellectual property in economic downturn

Even as the threats increase, the investments to protect intellectual property do not appear to be increasing in the countries hosting most of the intellectual property. In fact, an alarming percentage of respondents will decrease spending on protecting their vital information as a result of the ongoing financial situation, ranging from 14 percent in China and Dubai to 31 percent in Brazil.

Experts believe the biggest problem is that many companies continue to view security as a cost center, and the emphasis on cost centers is often decreased in the face of downturn. This is leading to an increasing number of potential easy targets for organized cybercriminals while the criminals themselves are improving the sophistication of their attacks.

According to respondents, it costs an average of almost $600,000 per firm to respond to each security breach concerning the loss of vital information such as intellectual property, and that number is expected to rise as the global recession drags on. It is worth nothing that this figure reflects just the cost of cleanup such as legal fees, victim notifications, not prevention and detection.

The research revealed that respondents worried more about the damage leakage or loss of vital information would do to their company's reputation than about the financial impact. Fifty percent of respondents said they worried more about the impact on reputation of data loss over the economic (33 percent) and the regulatory (16 percent) impact.

A HIGH PRICE TO PAY

Companies lost on average $4.6 million worth of intellectual property in 2008

Respondents reported losing intellectual property worth an average of $4.6 million per firm due to security breaches. This ranged from a low of $375,000 in the U.K. to a high of $7.2 million in China. The financial services industry suffered the highest losses with a $5.3 million per firm loss, followed by product development and manufacturing with a $4.6 million per firm loss in the past year. The total loss of intellectual property among respondents during the last 12 months excluding losses due to piracy came to $559 million.

CASE STUDY: Tele Atlas North America provides digital maps and other content for use in navigation systems and location-based services. Tele Atlas North America's health plan administrator, Willis North America, reportedly "misplaced" backup tapes containing employee data of Tele Atlas North America while the tapes were on their way to a storage facility on June 9, 2008. It was not disclosed whether the tapes were encrypted, although it is likely that they were not.

The tapes contained sensitive personal information on Tele Atlas North America's employees and their dependents, including names, addresses, birthdays and social security numbers. While it is unclear how many records were on the misplaced tapes, Tele Atlas North America had approximately 1700 employees at the time of the loss.

While Tele Atlas North America and Willis North America are both based in the United States, the tapes were on their way to a storage facility near Mumbai, India. It is not clear if the tapes have been found or if the data on the tapes is being used illegally. However, given the value of the data on the tapes, it is a distinct possibility that the information could fall into the wrong hands.

KEY FINDING 2:

The Current Economic Downturn May Be A Perfect Storm for Security Breaches

The global economic crisis is poised to create a "perfect information security storm" as increased pressures on firms to reduce spending and cut staffing have led to more porous defenses and increased opportunities for cybercriminals.

Respondents are clearly worried about the financial crisis and its impact on the security of critical information, such as intellectual property and sensitive information. Thirty-nine percent of respondents believe this information has become more vulnerable now due to the current economic climate.

Data thefts by insiders tend to have greater financial impact given the higher level of data access. When combined with the affect of today's economic realities on IT security spend, this could mean even greater financial risk to corporations.

The research shows that economic distress will exacerbate security issues for several reasons. Insider threats will still be a concern, and mass layoffs will incite a percentage of previously loyal employees to look at criminal activity. These economic realities could tempt an increasing number of financially strapped and laid-off employees to use their corporate data access to steal vital information. After all, who knows better where the goods are and how to get them than people with some connection to the organization?

Such predictions are supported by those surveyed, with 68 percent of respondents citing "insider threat" as the top threat to vital information. This was *above* patching vulnerabilities (51 percent), cyberterrorism (38 percent) and industrial espionage (36 percent).

Forty-two percent of respondents said laid-off employees are the biggest threat caused by the economic downturn, followed by outside data thieves (39 percent). Thirty-six percent were worried about the security threat from financially strapped employees. German respondents were most concerned with layoffs (70 percent) as were Brazilian (59 percent) and U.S. respondents (46 percent).

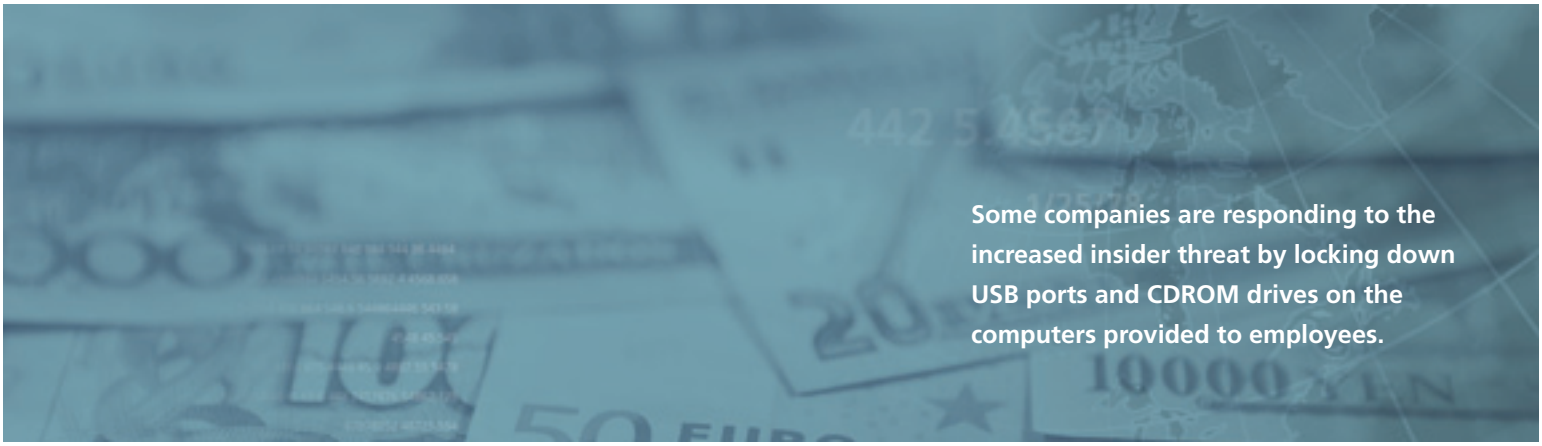
"Managing insider threats is difficult," said Tim Shimeall, an analyst at Carnegie Mellon University's CERT Network Situational Awareness Group or CERT/NetSA. "With more sophisticated technologies at their fingertips and increased access to data, it has become easier for current employees and other insiders, such as contractors, consultants, suppliers and vendors, to steal information."

Data thefts by insiders tend to have greater financial impact given the higher level of data access. When combined with the affect of today's economic realities on IT security spend, this could mean even greater financial risk to corporations.

Financial gain or competitive advantage: vital information becomes sought after currency for employees

With growing personal economic pressures, the threat from employees or ex-employees is higher because they have much greater incentives—as well as access to specific information—to create havoc. The insiders who steal data do so in some cases for financial gain, but for others, it's a way to

Forty-two percent of respondents said laid-off employees are the biggest threat caused by the economic downturn, followed by outside data thieves (39 percent).



Some companies are responding to the increased insider threat by locking down USB ports and CDROM drives on the computers provided to employees.

improve their job opportunities with the competition. The competitive advantage may play out even more as employees who may fear layoffs start to seek "backup" jobs at competitors, with the plan to entice the potential new employer with existing knowledge—and even data—from their current employer. They may also start companies of their own with the insight they gain. "The current economic situation has potential for laid-off employees to start up companies using the stolen information," said Rento Opice Blum, a Brazilian lawyer and professor.

Case after case shows the growing threat from insiders, both prior to and during the economic crisis currently facing the world.

Companies take drastic steps to lock down information

Some companies are responding to the increased insider threat by locking down USB ports and CDROM drives on the computers provided to employees. This technique is used by many Indian IT companies, as well as all over the world. Other extreme measures include requiring managers to be copied on all email sent outside the organization and monitoring print queues for potential leaks by employees.

Such drastic measures often reduce productivity and actually can cost companies more in resources than simply imposing the right policies, enforcing those policies and using the right protection security solutions.

CASE STUDY: In an example of data theft for competitive gain at a new competitor, an employee at Acme Tele Power Private Limited, an India-based company, allegedly leaked the software component of Acme's patented product, Power Interface Unit (PIU), to Lambda Eastern Telecom, Acme's competitor, in June 2006. Soon after the leak, the employee left Acme and joined Lambda, reportedly for a large pay increase. Acme claims that Lambda developed its product, BTS Shelter, based on the stolen research and development (R&D).

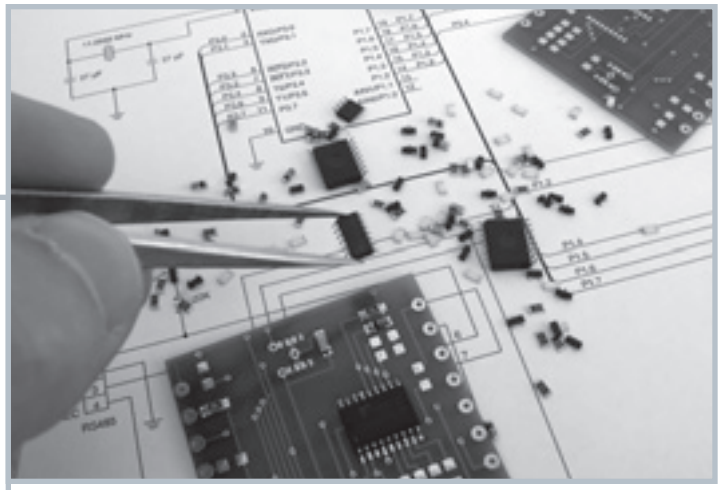
Acme alleges that Lambda could not have made their product in such a short period of time without illegally using Acme's intellectual property. The police were called to investigate and did eventually arrest the accused employee, although he was later released on bond. The role of Lambda in the incident remains unclear. Acme later moved its $10 million R&D operations to Australia, in hopes of finding a more business-friendly intellectual property protection environment.

CASE STUDY: In one example of data theft, FBI agents arrested Rene Rebollo, of Pasadena, CA, in August 2008. The former Countrywide Financial senior financial analyst was charged with downloading two million customer records to a flash drive and selling the data to identify thieves.

Rebollo had worked as a senior financial analyst at Full Spectrum Lending, the subprime lending division of Countrywide. He allegedly downloaded approximately 20,000 customer records at a time. He would download the records on Sunday evenings from an office computer that was lacking the security features of the other computers in the office. He would then sell these records for $400 to $500 a batch as mortgage prospects to agents of other firms via his accomplice, Wahid Siddiqi, who would act as the reseller of the data.

It appears as if the data was used to drum up new mortgage business for other companies, instead of outright identity theft, although the true scope is still unknown. The U.S. Attorney General's office stated that it appears that Rebollo sold the records for about $0.025 apiece, far less than their value at a legitimate data broker and even much less than the records would fetch on the black market.

The Rebollo case can be directly attributed to the downfall of the subprime mortgage industry. Other cases will undoubtedly follow as unscrupulous and now financially desperate employees (and ex-employees) seek to improve their financial situations at the expense of customers.



CASE STUDY: In another case of data theft in June 2008, a former Intel Corporation employee allegedly downloaded one billion dollars' worth of confidential intellectual property documents before leaving the company to join AMD, a competitor.

The U.S. Federal Bureau of Investigation (FBI) found more than 100 pages of sensitive documents and 19 computer-aided design (CAD) drawings of future processor chips at the home of the accused. The U.S. Department of Justice and the FBI was called after another Intel Corporation employee learned that the accused had started working for AMD before terminating employment with Intel, and that sensitive information had been accessed during that time frame.

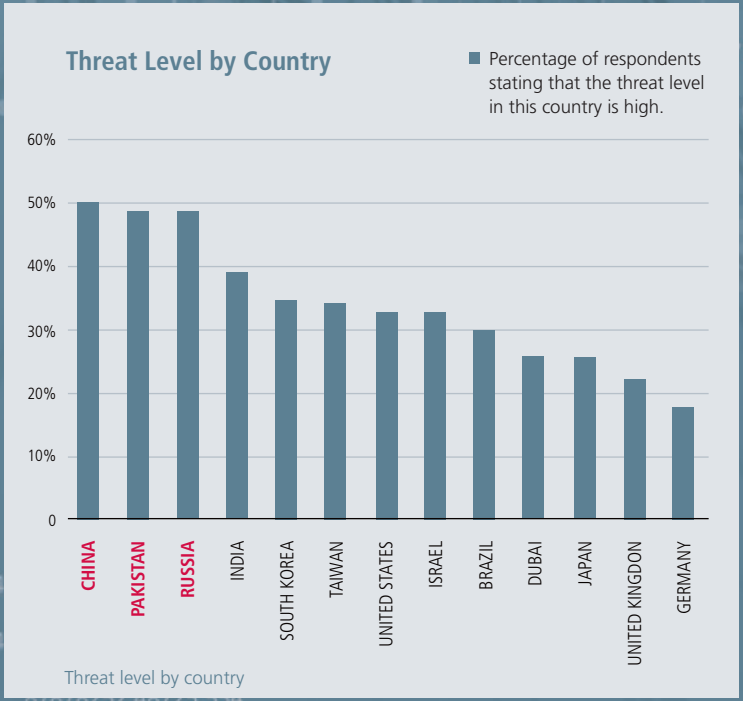
The former employee was charged in September 2008 with five counts of stealing trade secrets and wire fraud. He faces up to 90 years in prison if convicted on all counts.

AMD did not use the information, but another company may not have been so ethical.

KEY FINDING 3:

Geopolitical Perceptions Have Become A Reality in Information Security Policies

Certain countries are emerging as clear sources of threats to sensitive data, in particular to intellectual property. It appears that geopolitical perceptions are influencing data policy reality, as China, Pakistan and Russia were identified as trouble zones for various legal, cultural and economic reasons.



Respondents cited China, Pakistan and Russia as the worst-rated countries when it comes to the protection of digital assets.

China, Russia, Pakistan pose biggest threats-to vital information

Three countries, in particular, stood out to the survey respondents—perhaps reflecting broader security perceptions. Respondents cited China, Pakistan and Russia as the worst-rated countries when it comes to the protection of digital assets.

Pakistan, China and Russia, in that order, were also perceived to have the worst reputations for pursuing or investigating security incidents. Respondents cited corruption among law enforcement and the legal systems as well as poor skills among law enforcement as top reasons for the reputation rating.

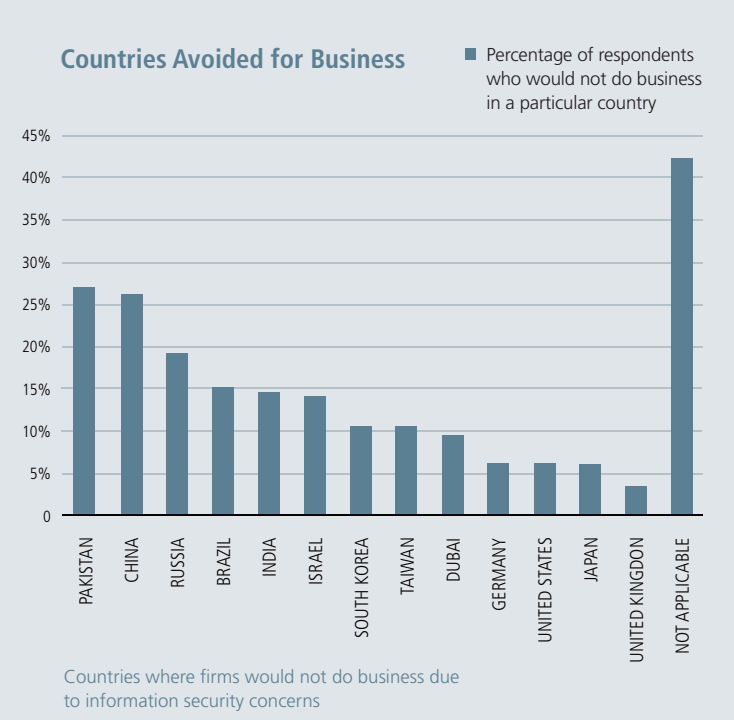
- **Perceptions among respondents may be rooted in both historical conflicts and modern economic, cultural and political differences.** Responses can be sorted according to long-time tensions between China and Japan, India and Pakistan, the U.S. and Russia, the U.K. and Russia, as well as more modern conflict between China and Taiwan and China and the U.S. According to Professor Takefuji at Keio University and an advisor to Japanese National Security Association, "In Japan, data leakage by employees is the biggest threat."
- **Chinese and Japanese respondents are suspicious of the information threats in the other's country.** For example, when asked to rate the threat level of various countries, 47 percent of Chinese respondents chose the U.S., followed by Taiwan (41 percent). Japanese respondents chose China (57 percent) followed by Russia (44 percent). Indian respondents overwhelmingly chose Pakistan (61 percent) as having the highest threat level. U.S.-based respondents chose China (62 percent) followed by Russia (59 percent). U.K.-based respondents selected Russia (74 percent) followed by Pakistan (68 percent) and China (66 percent).
- **Chinese respondents (42 percent) pointed to the data privacy protection in Japan's legal system as being the primary source of threat to sensitive data, while Japanese respondents (30 percent) identified the intellectual property protection in China's legal system as the primary source of threat.** Japanese respondents rated China as being ill-prepared to defend against threats (69 percent), with culture of the country being identified as the primary reason why the country is ill-prepared (38 percent).
- **The threats in China and, to a lesser extent, India, are of concern to U.S. companies, but Indian and Chinese respondents rate threats lower in each others' countries.** For example, Indian respondents rated China as less than a threat to sensitive data than Pakistan (38 percent versus 61 percent), and Chinese respondents rated India as less of a threat (38 percent) than the U.S. (47 percent), Taiwan (41 percent) and the same as Japan (38 percent). While Chinese respondents reported that they most avoid India due to intellectual property concerns (24 percent), far fewer Indian respondents would avoid China (11 percent).

In almost all the countries, ratings from other countries were worse than what the country perceived its own risk would be. The main exceptions are Japan and the U.S. Both Japanese and American companies rate their countries as higher risk

than how the world perceives it. Japan perceives itself to be a higher risk (15 percent) than the rest of the world (12 percent). The U.S. rates itself as a higher risk (21 percent) than the rest of the world (18 percent).

Countries are avoided for business due to security concerns

Yet, as a result of the mistrust, some companies completely refuse to produce their products in or transfer their intellectual properties to countries they believe pose a threat. A sizeable number of respondents reported that they avoid processing information in certain countries, particularly Pakistan, China and Russia, due to intellectual property and/or data privacy concerns.



Countries where firms would not do business due to information security concerns

Twenty-six percent of respondents had purposely avoided storing and/or processing data in China.

China

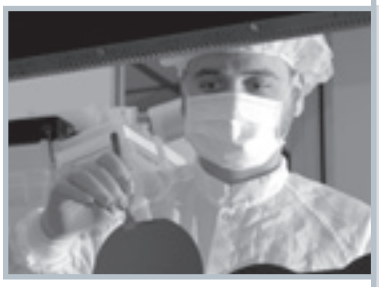
Twenty-six percent of respondents had purposely avoided storing and/or processing data in China.

Respondents pointed to both the lack of privacy and intellectual property protection as the primary reasons why China's threat to sensitive data was so high.

Like many developing economies, China's growth has far outpaced its ability to create and enforce legislation or—even more importantly—cultural attitudes toward protecting digital privacy and sensitive data. For example, the China Compulsory Certification (CCC) process has been identified as one technique used by the Chinese government to appropriate intellectual property. The certification requires companies wishing to sell electronic components in China to submit drawings, schematics and the finished product to the Chinese governmental body overseeing the certification.

"China is a large developing nation," said Shimeall of Carnegie Mellon University. "They are people rich but not resource rich. They are eager to develop the economy. The cheapest way, not necessarily the ethical way, is to indulge in industrial espionage. This is a concern with respect to other developing countries like India and Brazil also. Professor Heejo Lee at Korea University in Seoul noted several recent incidents targeting South Korean companies that could be traced to China-based hacking rings.

CASE STUDY: The trend to outsource manufacturing is well documented and has been driven by the basics of supply chain optimization—cost, flexibility and speed. Over the past couple of decades we've seen the rise of global manufacturing powerhouses like Mexico, China and South East Asia and a dramatic decline in traditional manufacturing jobs in locations like the U.S. and Western Europe. But concern about a company's ability to protect its core data—its intellectual property—can override even these powerful global economic forces.



A couple of years ago, a leading contract manufacturer established a manufacturing center for medical devices in Singapore. They chose that location for several key reasons—strong logistics, access to relatively affordable talent and a strong legal and cultural infrastructure of data protection. Clients of this manufacturer had made themselves perfectly clear—they wanted the lowest total landed cost, but were simply not willing to risk losing their IP by having the key components of their devices manufactured in China. Make the boxes and commodity pieces in China—but build the brains and do finally assembly in Singapore, even though it meant significantly higher costs.

– Former executive of a leading global contract manufacturer

Professor Katsuya Uchida of the Institute of Information Security, Japan, who is an assistant to CIO at the City of Yokohama, pointed out that in the institute's independent survey in 2006, about 64 percent of respondents blamed China for their intellectual property theft.

Pakistan—a cyberthreat? Myth or reality?

The survey results also indicate Pakistan is not a trusted place to do business. Twenty-seven percent stated that they have purposely avoided storing and/or processing data in Pakistan.

Pakistan's outsourcing industry is nowhere near as developed as its neighbor India. But the country has a reputation as a haven for hackers or cyberfraudsters, as do the former Soviet Republic countries, Eastern Europe and Nigeria.

Pakistan is suspected of harboring members of the Taliban and Al-Qaeda. This view may have contributed to the perception expressed by respondents that it poses a great risk to the integrity of critical data and is a country to which respondents would not consider outsourcing sensitive information and intellectual property.

"Pakistan has very good universities that are full of smart individuals, but unlike Iran, it is less isolated" said Lynn Robert Carter, associate teaching professor at Carnegie Mellon University in Qatar. "However, there is still extreme fundamentalism there with a high unemployment rate; even among the highly educated. This combination results in threats to information security on many levels."

Russia's cybermafia

Nineteen percent of survey respondents have purposely avoided storing and/or processing data in Russia.

According to Tim Shimeall of Carnegie Mellon University, the biggest source of threat in Russia is its mafia. "They have immense resources and proved to be ruthless. It is stated that eight percent of the world's deposits is owned by them. With resources like that, the mafia can build its own communication infrastructure. Obviously, managing attacks from such a resourceful criminal organization is quite difficult. The mafia has targeted bank access numbers, bank transfers, etc.," he said.

Pakistan, China and Russia, in that order, were also perceived to have the worst reputations for pursuing or investigating security incidents. Respondents cited corruption among law enforcement and the legal systems as well as poor skills among law enforcement as top reasons for the reputation rating.

CASE STUDY: An Indian software developer looking to improve a client's code posted a portion of it on the Internet to seek input from the development community without realizing that this action compromised the confidentiality of the client's intellectual property. While the developer's efforts to improve the code were sincere, the end result could have been quite damaging for the client.

According to 18 percent of Indian respondents, regulations exist to protect information assets but are not enforced.

India

India's reputation as a less-favored place for storing and/or processing data may be due to the attention-grabbing headlines when they began increasing their outsourcing operations for many countries. These headlines have undoubtedly made many companies nervous.

With such headlines, certainly, cases do exist in which companies have opted not to do business in India: a Canadian mobile weighing machine company refused a request from an Indian company to manufacture and market the product in India primarily because of intellectual property concerns.

Different cultural attitudes

Culture influences attitudes toward the value of intellectual property. Third and second world countries may be quite willing to say the intellectual property of others isn't worth protecting if it helps improve economic conditions at home. There are also differences across firms regarding protecting different types of intellectual property.

Professor Heejo Lee of Korea University pointed to a number of data breaches and privacy violations at Auction and other large Korean firms. He said that these incidents are considered intellectual property issues as defined by the Korean culture. However, many U.S.-based firms might classify this data as sensitive but may or may consider it intellectual property.

"Culture is a key problem," said Sivarama Krishnan, a partner with PricewaterhouseCoopers and based out of India. He pointed out that Indians and Americans have differing notions of privacy. For example, salary information is openly discussed among peers in India, but that is not the case in the United States. Indian companies dealing with American companies and their data must be sensitive to such issues and should provide adequate training and education to employees, suppliers, contractors, and even clients.

CASE STUDY WITH A TWIST: Some companies are intentionally exposing themselves to the threats. Heavy manufacturing is very dependent upon research and development in order to introduce new products in a highly competitive marketplace. Given the stagnant growth in the U.S. and the Western Europe, many heavy manufacturers were forced to consider developing markets such as India and China. Cummins, Inc., went so far at to open a research and development center in Wuhan, China. While it is possible that Cummins could lose some control of their IP by entering those markets, they made their decisions based on their strength of reputation and ability to innovate faster than an upstart company. So far this bet is paying off.

CASE STUDY: India received attention-grabbing headlines when a British newspaper did an undercover operation to secure contact details about British citizens from Indian call center employees. This incident also helped create awareness among call center employees about Western perspectives on privacy being different than those held in India.

Lax enforcement

Another concern for many regional respondents is the enforcement of policies. According to 18 percent of Indian respondents, regulations exist to protect information assets but are not enforced.

Brazil was rated by respondents, along with Pakistan, as the most ill-prepared to defend against threats by respondents. According to Renato Opice Blum, "The main problem is that Brazil's enforcement and judicial systems are too immature to deal with information threats. Brazilian laws do not specifically target information crimes and, hence, companies have to rely on laws designed to address traditional crimes of a more physical rather than virtual nature. This means that the burden of the proof is much higher. For example, the victim not only has to prove that the attacker entered a privately owned network but also that the attacker created damage. The proof of loss in the digital context is more difficult and therefore, the burden of proof is higher."

"While the U.K. and E.U. have stricter laws, the U.S. laws are better thought-through," said Professor Lilian Edwards of the University of Southampton. "In the U.K., for example, the law has to be enforced by an independent commission. However, the commission is ill-funded with little ability to enforce. On the other hand, laws in the U.S., such as HIPAA and financial reporting laws, are specific and targeted at the problem."

Interestingly, Indian and Chinese companies appear to be worried about the strict U.S. laws. Similarly, Indian companies are particularly concerned with strict privacy laws in U.K. but not about similar laws in Germany.

Vietnam and the Philippines perceived favorably—for now

The research indicates that Far East countries, such as Vietnam and the Philippines, are viewed favorably in the industry. A partner with Accenture (which has an offshore center in the Philippines) pointed out that while the salaries of IT employees in India have seen double-digit growth, the company has found a good balance between technology know-how and cost in these other countries.

A semiconductor executive who expressed reservations with China also pointed out that, even though the IP laws are not strong in Vietnam and the Philippines, the intellectual property problems are not as severe as in China. With careful attention from their governments, these countries have great potential to become intellectual property destinations.

Purdue's Professor Eugene Spafford, who is a leading information security expert, expects that these advantages will be short term. When the volume of intellectual property in these regions increases, he believes the criminals will be motivated to target them as well.

KEY FINDING 4:

Intellectual Property is a New Currency for Cybercriminals

"Before, criminals used to steal money to become rich, but now they have realized that they can be rich by stealing corporate information."

– US Treasury Department official

Cyberthieves have expanded their activities beyond basic hacking and stealing of credit card data and personal credentials. Their emerging target is intellectual property. *Why sink all that time and money into research and development when you can just steal it?*

Credit card fraud and identity theft have moved into the so-called "cash cow"[1] phase of criminal strategy. In other words, it's a source of revenue, but there's not much room for growth, so criminals are looking for the new stars of their portfolios. And intellectual property has emerged as a favorite.

[1] See the Boston Consulting Group's (BCG) matrix on product life cycles at www.bcg.com.

As cybercriminals realize just how valuable corporate information can be, they will push harder and harder against known vulnerabilities. Globally, the nature and sophistication of the attacks is evolving. This corresponds with the finding that patching vulnerabilities was the second biggest concern among respondents.

Attacks from data thieves was cited as a threat by 39 percent of respondents. Japanese respondents were most concerned about the threat from outside data thieves (70 percent), as were Chinese respondents (56 percent).

Despite this concern many companies, are leaving themselves open to exploitation and attack because they don't realize the value and location of their intellectual property. Some of that property is stored in Microsoft Word and Adobe Acrobat PDF documents, Microsoft PowerPoint presentations and other media formats. According to Ashish Arora of Duke University, it is becoming easier for hackers and others to attack intellectual property because data is increasingly codified and left on servers.

"We are noticing an increase in corporate data intrusions for purposes of gaining internal corporate data. As organized criminals, including mafia-style organizations, become involved in cybercrime, it is clear that the stakes from stealing the intangible assets are quite high." said Tom Longstaff, a former deputy director at CERTA and currently at Johns Hopkins University's Applied Physics Lab.

Cybercriminals invest in R&D and create test centers

The tools available to the cybercriminals are also becoming increasingly sophisticated. Fifty-four percent of respondents cited the changing nature of threats as a key challenge. Professor Ross Anderson of the University of Cambridge noted that malware writers now have R&D departments and test departments.

Attacks from data thieves was cited as a threat by 39 percent of respondents. Japanese respondents were most concerned about the threat from outside data thieves (70 percent), as were Chinese respondents (56 percent).

CASE STUDY: Industrial Espionage in South Korea [2]

Four Korean nationals were charged by Korean State Prosecutors with attempting to leak wireless and broadband Internet technology to the United States. The four are three former employees and a current researcher with POSDATA Co. Ltd., a computer services unit of Korea's number one steelmaker POSCO Co. The three former employees are currently U.S. green card holders and are undergoing extradition proceedings to Korea.

WiBro, short for wireless broadband, is a wireless Internet broadband technology developed by Korean telecommunications firms. It is capable of faster data transfer speeds than existing mobile technologies. Commercial WiBro service began in Korea in June of 2006 and helps increase data transfer rates among mobile devices, such as cell phones. A U.S.-based firm had planned to purchase the data being sold by the four and had already acquired some data identified by prosecutors as "non-core information". The four had planned to sell the information to the U.S.-based firm for 180 million won ($193 million U.S.D.) as well as lure away 30 key researchers as POSDATA for jobs at the U.S.-based firm. POSDATA spent 90 million won to develop the technology.

[2] "Four Indicted for Attempt to Leak WiBro Technology" *The Korean Herald,* May 21, 2007.

CASE STUDY: Industrial Espionage in Singapore [3]

SMC Marine Services, Pte., Ltd., is a Singapore-based bulk transporter of coal, gypsum, sand and other aggregates using tugboats and barges between Indonesia, Vietnam, Thailand and the Philippines. The company has accused a former systems engineer, Mr. Thangavelu Boopathiraja, of secretly setting passwords within a system that he developed for the company. Mr. Boopathiraja developed a real-time vessel-monitoring system that was supposed to send information on fuel usage and other key metrics from the ships back to corporate headquarters in Singapore. The system included hardware installed onboard the vessels, which requires codes to function. The same software that is used to write the codes also allows for password-protection features to be incorporated into the system, although the password feature is not installed by default. Mr. Boopathiraja left SMC soon after working on the system and started a competing company selling a similar vessel-monitoring system. Lawyers for SMC claim that employees are now unable to check, modify or upgrade the system. Mr. Boopathiraja is facing both criminal and civil penalties in the case.

[3] "Firm Takes Systems Engineer to Court; Former Employee is Accused of Setting Passwords that Access Program He Created" *The Straights Times (Singapore)* June 14, 2008.

CASE STUDY: Software maker Oracle sued its archrival on March 22, 2007 for industrial espionage. In November 2006, Oracle apparently observed heavy download activity on websites meant for customers using products from PeopleSoft and J.D. Edwards divisions, which Oracle had formed after acquiring the respective companies. The site, which had limited access rights, contained details regarding patches, instructions and software updates. Many of those downloads, according to the lawsuit filed in U.S. Federal District Court in California, were from an IP address at SAP's subsidiary TomorrowNow. TomorrowNow sold technical support for products from PeopleSoft, J.D. Edwards and Siebel, all of which were subsequently acquired by Oracle. Oracle alleges that employees at SAP logged on to Oracle's website by posing as customers with expired or soon-to-be-expired rights, including companies such as Honeywell International, Merck and Metro Machine Corp. By tracking the website log file, Oracle estimates that the more than 10,000 unauthorized software and support materials for various products were downloaded. From this allegedly stolen material, Oracle is concerned that SAP has gained intelligence to entice Oracle's customers to its own products and may also have improved its software.

In many companies, information technology people do not talk to legal counsel on this subject, and no one realizes the stake that the other has on this issue.

Malware such as MPack is regularly updated by its developers as to which vulnerabilities to exploit, much like system security products are updated with information regarding which vulnerabilities should be addressed.

Companies have been slow to respond to this new level of sophistication. According to Nick Akerman, a New-York based computer abuse and fraud lawyer with the firm Dorsey & Whitney, "Companies don't have an integrated solution to the problem, and they often treat human resources policies, information security and compliance programs separately. In many companies, information technology people do not talk to legal counsel on this subject, and no one realizes the stake that the other has on this issue."

Executives targeted by phishing attacks

Cybercriminals are targeting executives using sophisticated techniques such as phishing. Phishing has evolved from error-ridden fake emails to highly sophisticated and targeted "spear phishing" attacks, where even highly trained security professionals can have difficulty distinguishing a phishing email from a legitimate one. These attacks can be surprisingly effective. Spear phishing attacks are a weak point in many organizations' security programs, as it is easy for busy executives to not pay close attention and accidently give away user IDs and passwords in even poorly crafted attacks, let alone sophisticated ones.

Industrial cyberespionage on the increase

Experts agreed that if an enterprise can appropriate R&D at minimal cost compared to its competitor and the company can still produce a comparable product at a far lower cost, basic economics dictates that the firm will win in the marketplace. Therefore, the incentives for industrial espionage are high, particularly in highly sought-after developing markets, where many old economy firms might not be well established by brand reputation.

As companies in established economies invest millions, if not billions of dollars in research and development (R&D) activities, the dominant expectation has been that the investing parties should reap the rewards of any resultant success in the marketplace.

However, not all cultures embrace this philosophy, particularly in emerging economies such as China and Brazil. And not surprisingly, industrial espionage was identified as the fourth most serious threat by respondents interviewed.

Companies have been slow to respond to this new level of sophistication.

Cybercriminals are targeting executives using sophisticated techniques such as phishing.

Future Challenges and Recommendations

Future Threats

Having analyzed the current emerging threats to vital information like intellectual property, McAfee and experts from the Center for Education and Research in information assurance and security (CERIAS) in the United States believe the following three trends will make critical information more vulnerable.

Insider threat will grow

Business failures, mass layoffs, decimated markets and a poor economic outlook will lead to a vastly increased number of financially desperate current employees and laid-off staff stealing valuable corporate information, both for financial gain and to improve their job opportunities.

While the overall number of attacks by insiders has historically been reported as lower than those originating outside the firm, the average losses tend to be larger.

Combine this with companies acting very quickly, and thus possibly not having strong procedures in place to lock out accounts, not performing regular internal audit and not taking other actions to avoid attacks, and it is clear that companies are continuing to put themselves at great risk.

Additionally, increasing merger and acquisition activity will expose firms to greater risk while systems integration is underway.

Michael Versace, senior advisor at Financial Services Technology Consortium, says, "For example, when two companies merge, or if two businesses of the same company are consolidated, one challenge that should be top of mind is to establish and implement a common or shared information governance policy. Given the profile of many of the financial institutions in the news today and global economic downturn, criminals and others are ready to exploit a potential lack of focus on risk management and poorly designed and/or implemented information governance and security policies."

More sophisticated and targeted attacks from cybercriminals

Criminals will devise increasingly sophisticated schemes to take advantage of employees, new technologies and software vulnerabilities.

Attackers will put together increasingly detailed and sophisticated profiles of executives and other targets in order to take spear phishing attacks to the proverbial "next level."

Attackers will comb blogs, press releases, magazine and newspaper articles, corporate information databases and social networking sites to gather details of executives' public and private lives in order to gain access to user IDs, passwords, financial and systems account information and other sensitive corporate data (also known as gathering "open source intelligence").

Web 2.0 technologies and "cloud computing" where people collaborate, share and use existing components to build new applications will create an environment of great innovation but can also create a back door for cybercriminals to steal sensitive data.

Geo-information "hot zones"

As China and Russia's economies soften, there will be even more pressure to "appropriate" intellectual property as a means to continue economic growth. Organized crime and state-sponsored groups in both Russia and China will continuously seek out new and profitable targets. Pakistan looms as potentially the largest threat, with attackers motivated by ideology rather than economic gain.

Expert Recommendations

In a world where trade barriers are lowered but criminal and civil codes and enforcement for cybercrime are still geographically constrained, and cybercrime grows in sophistication, there is a need for a unified approach that helps companies protect their vital information.

Companies must also adopt a different attitude towards protecting their vital information and how they value their vital information "assets."

EXPERTS RECOMMEND THE FOLLOWING STEPS

Define an internationally adopted protocol for dealing with corporate cybersecurity incidents

Not only do different countries have different laws and different attitudes to enforce existing laws, but often criminals and victims reside in different jurisdictions, so the perpetrator of the crime able to cause significant damage without ever physically entering the victim's premises.

While detecting crime against sensitive data and intellectual property can be difficult in certain circumstances, identifying the perpetrator, extraditing and successfully prosecuting are often practically impossible.

Experts believe that while the Council of Europe Convention on Cybercrime goes a long way in addressing some of these issues, there is still too much flexibility in interpreting and implementing the provisions. Additionally, the lack of ratification by many countries limits the overall effectiveness of such efforts.

Dr. Marco Gercke, Lecturer for Law related to Cybercrime at the University of Cologne, Germany, suggest that nations need to ratify the Council of Europe Convention on Cybercrime and fully embrace its provisions.

He also noted that in many ways, Eastern Europe is much better prepared than Western European countries to enforce the provisions of the Convention. Many Eastern European countries, such as Bulgaria and Romania, have signed and ratified the Convention, whereas Germany and the U.K. have signed but not ratified the Convention. The U.S. has both signed and ratified the Convention, as of January 1, 2007. Canada, Japan and South Africa have signed but not ratified the Convention. Russia has refused to sign the Convention, citing disagreement on terms for cross-border access to data processing networks.

Dr. Gercke also points out that the Convention needs to be updated to reflect increasing sophistication on the part of cybercriminals, as well as the ongoing innovation in technology itself.

Criminals will devise increasingly sophisticated schemes to take advantage of employees, new technologies and software vulnerabilities.

CASE STUDY: In October 2007, Oleksandr Dorozhko, a Ukranian citizen, breached the systems of Thomson Financial, a US-based publisher of business information. The breach was initiated from a computer in the Ukraine. Mr. Dorozhko allegedly read a report detailing negative news about IMS Health, a company listed in the NYSE, that was not intended for immediate public consumption. It was anticipated that this negative news regarding IMS Health would result in a drop in IMS Health's stock price once it was made public. Mr. Dorozhko was able to capitalize on this news by immediately selling "put options" on IMS Health resulting in a $300,000 gain (a "put option" is an option contract giving the holder the right to sell a certain quantity of a stock at a specified price by a given date.) The Securities Exchange Commission (SEC) attempted to freeze the proceeds but a judge responding to a counter suit from Dorozhko agreed that hacking did not violate insider trading law, thus allowing him to keep the proceeds. It is agreed that he broke the law while into breaking into the network. But the New York Times speculates that because of the difficulties in gaining cooperation from the local authorities, the chances of extraditing him from the Ukraine to face those charges are slim.

Sivarama Krishnan of PriceWaterhouseCoopers, suggests an alternative approach—an internationally accepted set of protocols for defining acceptable and unacceptable activities, procedures for investigation and apprehension of suspects and sentencing guidelines that would streamline and thus result in much greater effectiveness in prosecuting international cybercrime cases.

Krishnan highlights the International Air Travel Association's (IATA) protocols for arriving and departing aircraft as a possible model for such protocols. The IATA protocols are followed regardless of the nationality of the airline, primary language spoken by the airline crew and the country in which the aircraft is landing and departing.

Companies must adopt a different attitude toward protecting their informational assets

Experts such as Michael Versace, senior advisor at Financial Services Technology Consortium (FSTC), Versace, say that companies have to shift their mindset in the way they value vital information and how they secure it.

Versace says that companies must expand their view of information governance and security policy beyond the perimeter and think strategically about the value of information assets in the extended enterprise, the related risk and risk mitigation techniques and prudent methods for managing and monitoring risks as part of day-to-day business operations.

Tom Longstaff, who was a deputy director at CERTS and is currently at Johns Hopkins University, says that, "Historically, companies have developed protection measures based on the intrinsic value of information. Given that it is very difficult to value informational assets, such an approach has inherent problems. Instead, the protection afforded to them should be based on how much it costs to generate that information. Some banks have already started adopting such a system."

"The intellectual property loss estimated is significantly less than the actual value lost. The realization that such losses are significant will take a few more years," explained Longstaff.

While many companies feel tremendous time pressure to reduce headcount and slash other expenditures, it remains critically important to carefully manage the human element.

Another expert, Ashish Arora, a professor at Duke University specializing in intellectual property explains the difficulty in valuing information assets such as intellectual property: "We have measures such as cost per square foot to generally assess the value of a house in a specific neighborhood. There is no such standardized way to assess the value of patents and other intellectual properties. It becomes difficult to assign appropriate risk-mitigation measures to those assets and therefore has the potential to leave significant gaps in the protection of these assets."

In India, CSOs from the leading Indian software companies (collectively known as SWITCH: Satyam, Wipro, Infosys, Tata, Cognizant, and HCL), have started to work together to deal with the common issues they face in protecting their vital information. They meet once every six months to discuss customer problems with respect to threats and process changes to addressthose threats.

Companies must pursue better employee education and closer alignment of human resources and IT

While many companies feel tremendous time pressure to reduce headcount and slash other expenditures, it remains critically important to carefully manage the human element. From developing carefully crafted severance procedures to carefully monitoring employee behavior, firms need to employ both educational tools, such as effective training, and technological controls to monitor their systems and protect against rogue behavior.

Employees at all levels of the firm must be trained, and the training must be regularly reinforced against the dangers of phishing and other social engineering attacks. Firms should set policies and educate employees about the dangers related to blogs, social networking sites and other places where content is publicly accessible. Furthermore, firms should partner with vendors to develop more sophisticated software and tracing tools to ensure the validity of all electronic communications.

"A firm can protect data and mitigate its risk by considering information security in the following seven areas of business: company rules; hiring practices to explain the rules and protect against data from competitors infecting the workplace; agreements with officers, employees and third parties memorializing data policies; the company compliance program; use of technology to enforce the rules and detect data breaches; employee termination practices and protocols for response to an attack" according to Nick Akerman.

Data loss in a downturn

At any time, but particularly in recessionary times, it's critical to be diligent about your intellectual property and valuable customer, citizen, or other corporate information. You may feel that your company is hurting now, but if you do suffer a breach, of any magnitude, it will only cost you more—at a time when you least need the additional costs. The following are but a few recommendations of what to do in this particularly volatile time.

- Write concrete contracts with specific security requirements for outsourcers
- Enforce those requirements
- Know the country's laws and their ability to enforce such policies in time of breaches
- Invest in the right solutions to protect data, but also invest in the employees—retain sufficient staff who understand where the data is housed, how it is protected and how to respond in a time of a breach
- Protect your accounts during layoffs to ensure that no one has access who is not on your active payroll
- Increase employee training and awareness
- Enforce policies with employees, helping them to understand the criticality of safe business practices

Employees at all levels of the firm must be trained, and the training must be regularly reinforced against the dangers of phishing and other social engineering attacks.

Conclusion

A single breach or loss of vital corporate information like intellectual property can impact the bottom line, share price and customer confidence virtually overnight. In the current economic downturn, the demand for illicitly gained intellectual property or other sensitive information will only increase as companies look to strip every possible cost from R&D and speed time to market of goods and services and cybercriminals look to improve their profits.

The vulnerability of vital information has increased as technology advances and information is distributed across networks of unsecured economies. The interconnected nature of the world's economies combined with growing economic uncertainty and piecemeal approach to cybercrime response will result in significant challenges for those charged with maintaining confidentiality, integrity and availability of vital information like intellectual property.

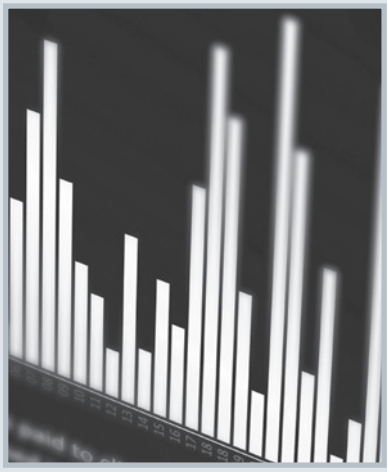
Professor Spafford of Purdue observes: "Information security has transformed from simply 'preventing bad things from happening' into a fundamental business component. C-level executives must recognize this change. This includes viewing cybersecurity as a critical business enabler rather than as a simple cost center that can be trimmed without obvious impact on the corporate bottom line; not all of the impact will be immediately and directly noticeable. In some cases, the only impact of degraded cybersecurity will be going from 'Doing okay' to 'Completely ruined' with no warning before the change."

He further stated "Cybersecurity fills multiple roles in a company, and all are important for organizational health.

- **First,** cybersecurity provides positive control over resources that provide the company a competitive advantage: intellectual property, customer information, trends and projections, financial and personnel records and so on. Poor security puts these resources at risk.
- **Second,** good security provides executives with confidence that the data they are seeing is accurate and true, thus leading to sound decisions and appropriate compliance with regulation and policy
- **Third,** strong cybersecurity supports businesses taking new risks and entering new markets with confidence in their ability to respond appropriately to change
- **And fourth,** good cybersecurity is necessary to build and maintain a reputation for reliability and sound behavior, which in turn are necessary to attract and retain customers and partners. This study show clearly shows that some customers are unwilling to do business with entities they consider poorly secured."

Professor Spafford continued, "Given massive market failures, significant fraud and increasing threats of government oversight and regulation, companies with strong controls, transparent recordkeeping, agile infrastructures and sterling reputations are clearly at an advantage—and strong cybersecurity is a fundamental component of all four. Executives who understand this will be able to employ cybersecurity as an organic element of company (and government) survival—and growth."

In conclusion, Professor Spafford notes, "This study shows that there is global awareness of cybersecurity incidents and cybercrime and a significant lack of trust in many areas. Our future will not be defined by those individuals who use results such as these to determine what to fear. Rather, our future will be defined by those leaders who see an agenda for positive action and who commit themselves to addressing the problems."



Professor Spafford notes, "This study shows that there is global awareness of cybersecurity incidents and cybercrime and a significant lack of trust in many areas.

CONTRIBUTORS

NORTH AMERICA:

Nick Akerman is a partner in the Trial group of Dorsey & Whitney LLP and co-chair of the Computer Fraud and Abuse practice.

He represents clients in trial and appellate courts and arbitrations throughout the United States. His specialties include: protection of trade secrets and computer data, complex commercial litigation, internal investigations and white-collar criminal representations. He is a former federal prosecutor, having served as an Assistant U.S. Attorney in the Southern District of New York and an Assistant Special Watergate Prosecutor with the Watergate Special Prosecution Force. He earned his J.D. from Harvard Law School in 1972 and is admitted to practice in New York and Massachusetts.

Dr. Ashish Arora, Ph.D., is a professor at Duke's Fuqua School of Management.

His research focuses on the economics of technology and technical change. Arora's research includes the study of technology-intensive industries such as software, biotechnology and chemicals; the role of patents and licensing in promoting technology startups and the economics of information security. Along with Alfonso Gambardella and Andrea Fosfuri, he authored *Markets for Technology: The Economics of Innovation and Corporate Strategy in 2001*. He served as a co-director of the Software Industry Center at Carnegie Mellon University until 2006. He has served on several committees for organizations, such as the National Academy of Sciences and the Association of Computing Machinery. He serves on the Advisory Committee on Measuring Innovation in the 21st Century to the Secretary of Commerce.

Gail F. Farnsely is currently a visiting professor in the College of Technology at Purdue University.

Prior to joining Purdue Gail was VP of IT and CIO at Cummins, Inc. In this role she had global responsibility for Information Technology at Cummins, including setting strategy and standards, applications development, implementation and support, and operations and infrastructure. Before her appointment as CIO, she worked in various IT roles, including spending two and a half years in the U.K., where she led the IT organization for the Europe, Middle East and Africa region, as well as Cummins' Power Generation IT globally. Prior to Cummins, Gail spent nine years with Georgia-Pacific in Atlanta, Georgia, worked as an Analyst at Emery Airfreight and began her career at Public Service Indiana (now part of Duke Energy). Gail began her career as a programmer and worked her way through the IT ranks, primarily in applications development and support organizations, with one foray outside of IT to lead a business process improvement project.

Karthik Kannan is currently an Assistant Professor of Management Information Systems in the Krannert School of Management at Purdue University and also a faculty associated with CERIAS.

He has master's degrees in electrical and computer engineering and public policy and management and a Ph.D. in information systems, all from Carnegie Mellon University. His two primary areas of research interests are the economics of information security and pricing of goods in information contexts. He has published papers in leading journals in information systems, including *Management Science* and *Information Systems Research*. His papers have appeared in many conferences and workshops, including Workshop on Economics of Information Security (WEIS), International Conference on Information Systems (ICIS), Workshop on Information Technology and Systems (WITS) and Workshop on Information Systems Economics (WISE).

Tom Longstaff, Ph.D., is the senior advisor for science and technology for the Applied Information Science Department of the Applied Physics Laboratory (APL), Johns Hopkins University.

Tom joined APL in 2007 to work with a wide variety of infocentric operations projects on behalf of the U.S. Government to include information assurance, intelligence and global information networks. Prior to coming to APL, Tom was the deputy director for technology for CERT at Carnegie Mellon University's Software Engineering Institute. In his 15-year tenure at CERT, Tom helped to create many of the projects and centers that enabled CERT to become an internationally recognized network security organization. His work included assisting the Department of Homeland Security and other agencies to use response and vulnerability data to define and direct a research and operations program in analysis and prediction of network security and cyberterrorism events. Tom's academic publications span topics such as malware analysis, information survivability, insider threat, intruder modeling and intrusion detection. He maintains an active role in the information assurance community and regularly advises organizations on the future of network threat and information assurance. Tom is on the faculty of The Johns Hopkins University and is a fellow of the International Information Integrity Institute.

Jacquelyn Rees is currently an associate professor of Management Information Systems in the Krannert Graduate School of Management at Purdue University.

She earned her Ph.D. in decision and information sciences from the Warrington College of Business at the University of Florida in 1998. Her research interests include information security risk management, privacy and evolutionary computation. She has published in journals

such as *Communications of the ACM, Decision Sciences, Decision Support Systems, European Journal of Operational Research, INFORMS Journal on Computing, Information Technology and Management, International Journal of Electronic Commerce* and the *Journal of Organizational Computing and Electronic Commerce.*

Dr. Timothy J. Shimeall, Ph.D., is a Senior Member of the Technical Staff with the Networked Systems Survivability Program at the Software Engineering Institute (SEI).

The CERT Coordination Center is also a part of this program, and Tim's work draws heavily on data from there. Tim is responsible for overseeing and participating in the development of analysis methods in the area of network systems security and survivability. This work includes development of methods to identify trends in security incidents and in the development of software used by computer and network intruders. Of particular interest are incidents affecting defended systems and malicious software that are effective despite common defenses.

Eugene H. Spafford is generally acknowledged as one of the senior leaders in information security. Spaf, as he is known to friends and colleagues, has been involved in research, education and the practice of IT security and reliability for over a quarter decade. He is a professor of computer sciences at Purdue University in the United States and is the founder and executive director of CERIAS. Dr. Spafford is a Fellow of the ACM, the IEEE, the AAAS, and the (ISC)^2. More information is available at http://bio.spaf.us

Michael Versace is currently Senior Advisor at Financial Services Technology Consortium (FSTC).

His accomplishments include the development and launch of FEDNET, the U.S. payments backbone network, the introduction of Internet and chip card payment schemes, the deployment of distributed cryptographic systems in ATM and POS networks and the design of generalized technology risk programs. He has held the position of Chairman and Vice Chairman of the International Standards Organization (ISO) technical committee on security for financial systems, Head of the United States Delegation to ISO, and Board Director for X9, Inc. and Program Executive with the Financial Services Technology Consortium. He has contributed to the development of numerous technical standards on cryptography, risk management and information security policy.

EMEA:

Dr. Ross Anderson, Ph.D., is Professor of Security Engineering at Cambridge University.

He is a co-founder of a vigorously growing new discipline: security economics. Many security failures can be traced to wrong incentives rather than technical errors, and the application of microeconomic theory has shed new light on many problems that were previously considered intractable. Professor Anderson has also made many technical contributions, having been a pioneer of peer-to-peer systems, hardware tamper-resistance, copyright watermarking and API security. He was a co-inventor, with Eli Biham and Lars Knudsen, of the Serpent algorithm which was a finalist in the Advanced Encryption Standard competition. He chairs the Foundation for Information Policy Research, the main U.K. think tank on Internet and technology policy issues. He is a Fellow of the IET and the IMA, and wrote the definitive textbook *Security Engineering—A Guide to Building Dependable Distributed Systems.*

Lynn Robert Carter has been a senior researcher and educator at Carnegie Mellon University for over nineteen years.

During his twelve years at the SEI, his work included onsite software technology adoption support to numerous military and commercial customers supporting the following technologies: real time schedulability, client/server system architectures, object orientation, process improvement and organizational change. After leaving the SEI, he established and supported the development and deployment of professional Software Engineering Masters programs at CMU West and with our partners at the SSN School of Advanced Software Engineering, Chennai, India and the International Institute for Information Technology, Hyderabad, India. He is now helping to establish an undergraduate software engineering track within the computer science degree program at Carnegie Mellon University in Qatar and working to establish professional masters programs at this new campus. His research focus is the adoption of new software technologies with a special focus on predictable and quality software development and management for high value systems. He has been active with computer science and software engineering accreditation for over eleven years and current serves as an ABET Commissioner and Executive Committee Member. Prior to Carnegie Mellon University he developed software, managed teams and lead research efforts at various commercial firms for 17 years, including: Tektronix, Motorola, GenRad and two startups. At GenRad, he led a leveraged buy-out of the data communications test equipment business and ran the spinout as its president and CEO. He earned his Ph.D. in Computer Science from the University of Colorado at Boulder in 1980 and his Bachelors and Masters in Mathematics with specialization in Computer Science from Portland State University in 1972 and 1974.

5 5622350479 658. 7895200.02. 33695 454868.45 5 48 4528782 45 4582 688.54 58 89 8 4568 44 822.656 546 78952 565.369 21
77787 4651

54868.45 5 48 4528782 45 4582 688.54 58 89 8 4568

4528782 45 4582 688.54 58 89 8 4568 44 822.656 54868.45 5 48 4528782 45 4582 688.54 58 89 8 4568 44 822.656

Lilian Edwards – Professor of Internet Law, University of Sheffield, U.K.

Lilian Edwards leads a program of research and teaching at Sheffield University focusing on the law relating to the Internet and new technologies. Her research interests are generally in the law relating to the Internet and communications technologies with a European and comparative focus. Her current research focus is on the role of intermediaries and ISPs on the Internet, privacy and data protection online, cybercrime and cybersecurity, Web 2.0 and the law, digital IP and e-commerce. She has co-edited two editions of her bestselling book on *Law and the Internet* (the third is due out in early 2009) and a third collection of essays *The New Legal Framework for E-Commerce in Europe.* Her work on online consumer privacy won the Barbara Wellbery Memorial Prize in 2004 for the best solution to the problem of privacy and transglobal data flows. She is an adviser to BILETA, the ISPA, FIPR, and the Online Rights Group, and has consulted for the European Commission and WIPO.

Dr. Marco Gercke is an attorney-at-law admitted to the German bar. He is teaching law related to cybercrime and European criminal law at the University of Cologne and is visiting lecturer for international criminal law at the University of Macau.

Marco is a frequent national and international speaker and author of more than 50 publications related to the topic of cybercrime. His main areas of research are international aspects of cybercrime (especially the challenges of fighting cybercrime and legal responses) and comparative law analysis regarding the implementation of international standards. Latest research covered the activities of terrorist organizations in the Internet, identity theft, money laundering on the Internet and legal responses to the emerging use of encryption technology. He is Secretary of the Criminal Law Department of the German Society for Law and Informatics, member of the ITU High Level Expert Group and works as an expert for the Council of Europe, the International Telecommunication Union and other international organizations.

LATIN AMERICA:

Augusto Paes de Barros has worked as an information security professional since 2000.

Since then he worked not only as a consultant but also as security executive. Augusto now works as Senior Information Security Specialist for one of the major Canadian banks in Toronto. He is constantly expressing opinions on different security subjects, especially through his blog, articles in specialized magazines and presentations at conferences around the world. He was also president of the Brazilian ISSA Chapter during 2006 and 2007.

Renato Opice Blum: Opice Blum Advogados Associados, Brazil

Opice Blum Advogados Associados has years of solid experience in the main areas of law, especially in technology, electronic law, information technology and its variations. As a pioneer in those matters, the company is also active in mediations, arbitration, oral sustaining in court, bio-law, typical technological contracts, cybercrime and other areas. It operates throughout the Brazilian territory and has international correspondents in the main international financial centers, such as Miami and New York.

As a member of several institutional organizations, the organization contributes to the evolution of the law related to technological development. It is outstanding as founding partner of the Brazilian Chamber of Electronic Commerce, member of the Computation Brazilian Society, among other institutions.

ASIA PACIFIC:

Sivarama Krishnan is currently an executive director at PricewaterhouseCoopers, Mumbai.

With more than 15 years of experience, he leads the Information Technology Risk Management and Security Practice in the firm. He has been dealing with projects in various countries including India, Kuwait, Bahrain, UAE, Oman, Sri Lanka, Bangladesh, the Netherlands, Singapore, the U.K. and the U.S. He leads a team of over 75 IT professionals and is an expert in areas including IT security, e-governance and telecommunication. Siva has hands-on experience in designing networks, implementation of e-governance applications and setting up IS, a management and security framework for large companies and governments. He is a chartered accountant by training and has been a visiting faculty to Institute of Chartered Accountants of India and Indian Institute of Foreign Trade, Delhi.

Heejo Lee is an associate professor at the Division of Computer and Communication Engineering, Korea University, Seoul, Korea.

Before joining Korea University, he was at AhnLab, Inc. as a CTO from 2001 to 2003. From 2000 to 2001, he was a postdoctorate at the Department of Computer Sciences and the security center CERIAS, Purdue University. Dr. Lee received his B.S., M.S., Ph.D. degree in Computer Science and Engineering from POSTECH, Pohang, Korea. Dr. Lee serves as an editor of the Journal of Communications and Networks. He has been an advisory member of Korea Information Security Agency and Korea Supreme Prosecutor's Office. With the support of Korean government, he worked on constructing the National CERT in the Philippines (2006) and consultation on cybersecurity in Uzbekistan (2007). More information is available at http://ccs.korea.ac.kr.

8 4568 44 822.656 546 78952 565.369 21
54868.45 5 48 4528782 45 4582 688.54 58 89 8 4568

5 4528782 45 4582 688.54 58 89 8 4568 44 822.656 54868.45 5

Professor Yoshiyasu Takefuji, Ph.D., has been a tenured professor on the faculty of environmental information at Keio University since April 1992 and was on the tenured faculty of Electrical Engineering at Case Western Reserve University since 1988.

Before joining Case, he taught at the University of South Florida and the University of South Carolina. He received his B.S. (1978), M.S. (1980) and Ph.D.(1983) from Electrical Engineering from Keio University under the supervision of Professor Hideo Aiso. His research interests focus on neural computing, security, internet gadgets and nonlinear behaviors. He received the National Science Foundation/Research Initiation Award in 1989 and received the distinct service award from IEEE Trans. on Neural Networks in 1992 and has been an NSF advisory panelist. He received the TEPCO research award from 1993 to 1995 and the Takayanagi research award in 1995. He also received the Kanagawa Academy of Science and Technology research award from 1993 to 1995. He has published several books and has served on the editorial boards of several journals. He has published more than 120 journal papers and more than 100 conference papers. He is included in *Who's Who in America, Who's Who in the Midwest* and *Who's Who in Science and Engineering, Men of Achievement.* He was an advisor to Multimedia University in Malaysia, PSDI of Philippine government, and VITTI (Vietnam Information Technology Training Institute), Srilanka, Thailand and Jordan CTTISC, respectively. He is an official assessor of the Hong Kong government.

Professor Katsuya Uchida, Ph.D., is a faculty member at the Institute of Information Security, Graduate school in Japan. He received his Ph.D. in science and engineering at Chuo University. He has been engaged in COBOL compiler development and user support at a small business computer dealer, EDP auditing and technical support for the electronic banking system at an American bank in Japan and an implementation project on computer insurance and information security research and study at a major non-life insurance company in Japan. Currently, he teaches information security management systems,risk management, and hands-on secure systems, at the Institute of Information Security. His main research topics are information security management systems, information security psychology, risk management and others. Dr. Uchida is a member of Computer Security Institute and a member of Information Processing Society of Japan. He is also an assistant to the CIO at the City of Yokohama.

Dr. Sun Yuqing, Ph.D., is currently an associate professor in the School of Computer Science and the director of the Department of Electronic Business Technology at ShanDong University.

Her research activities are related to various topics: access control model and technology; security policy; security in web services; workflow management; trust management and others. She has published more than twenty papers for international conferences and journals in recent years and is the PI of several projects, including the science foundation project and the Momentous Science Development Plan Program of Shandong Province. She writes reviews for many journals and has served on the program committees of many international conferences. Currently, she is serving on the program committees of ICESS'09, MUE'09, CIS'08, ICPCA08, SCC08, EDOC08, ICMLC08 ICESS08 MUE08 and others.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054

888.847.8766

www.mcafee.com

For PR inquiries and other
related questions, please contact:

Sal Viveros
McAfee, Inc.
+44 (0) 1753.217492 or +1.408.346.3696
Sal_Viveros@mcafee.com

Stuart Yeardsley
Red Consultancy for McAfee, Inc.
+1.415.618.8814
stuart.yeardsley@redconsultancy.com

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

http://www.mcafee.com

McAfee and/or other noted McAfee related products contained herein are registered trademarks or trademarks of McAfee, Inc., and/or its affiliates in the U.S. and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. Any non-McAfee related products, registered and/or unregistered trademarks contained herein are only by reference and are the sole property of their respective owners.

© 2009 McAfee, Inc. All rights reserved.

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. We endeavour to ensure that the information contained in the McAfee Unsecured Economies Report is correct; however, due to the ever-changing state of security the information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.