KPMG INTERNATIONAL

Issues Monitor

Cyber Crime – A Growing Challenge for Governments

July 2011, Volume Eight

kpmg.com

KPMG
cutting through complexity

John Herhalt

Global Chair, Government

Keeping up to date with the very latest and most pressing issues facing your organization can be a challenge, and while there is no shortage of information in the public domain, filtering and prioritizing the knowledge you need can be time consuming and unrewarding. I hope that you find *Issues Monitor* useful and we welcome the opportunity to further discuss the issues presented and their impact on your sector.

Welcome to the July edition of *Issues Monitor – Government on Cyber Crime*. Each edition pulls together and shares industry knowledge to help you quickly and easily get briefed on the issues that affect your sector.

Cyber crime – a growing challenge for governments

In a digital age, where online communication has become the norm, internet users and governments face increased risks of becoming the targets of cyber attacks. As cyber criminals continue to develop and advance their techniques, they are also shifting their targets — focusing less on theft of financial information and more on business espionage and accessing government information. To fight fast-spreading cyber crime, governments must collaborate globally to develop an effective model that will control the threat.

Introduction

> In 2010, the global spam rate increased 1.4 percent year-on-year, to 89.1 percent.

Advancements in modern technology have helped countries develop and expand their communication networks, enabling faster and easier networking and information exchange. Currently, there are nearly 2 billion internet users and over 5 billion mobile phone connections worldwide. Every day, 294 billion emails and 5 billion phone messages are exchanged. Most people around the world now depend on consistent access and accuracy of these communication channels.[1]

The growing popularity and convenience of digital networks, however, come at a cost. As businesses and societies in general increasingly rely on computers and internet-based networking, cyber crime and digital attack incidents have increased around the world.[2] These attacks — generally classified as any crime that involves the use of a computer network — include financial scams, computer hacking, downloading pornographic images from the internet, virus attacks, e-mail stalking and creating websites that promote racial hatred.[3] The first major instance of cyber crime was reported in 2000, when a mass-mailed computer virus affected nearly 45 million computer users worldwide.[4]

Table 1: Types of cyber attacks[5]

Type of attack	Details
Viruses and worms	Viruses and worms are computer programs that affect the storage devices of a computer or network, which then replicate information without the knowledge of the user.[6]
Spam emails	Spam emails are unsolicited emails or junk newsgroup postings. Spam emails are sent without the consent of the receiver — potentially creating a wide range of problems if they are not filtered appropriately.[7]
Trojan	A Trojan is a program that appears legitimate. However, once run, it moves on to locate password information or makes the system more vulnerable to future entry. Or a Trojan may simply destroy programs or data on the hard disk.[8]
Denial-of-service (DoS)	DoS occurs when criminals attempt to bring down or cripple individual websites, computers or networks, often by flooding them with messages.
Malware	Malware is a software that takes control of any individual's computer to spread a bug to other people's devices or social networking profiles. Such software can also be used to create a 'botnet'— a network of computers controlled remotely by hackers, known as 'herders,' — to spread spam or viruses.
Scareware	Using fear tactics, some cyber criminals compel users to download certain software. While such software is usually presented as antivirus software, after some time these programs start attacking the user's system. The user then has to pay the criminals to remove such viruses.[9]
Phishing	Phishing attacks are designed to steal a person's login and password. For instance, the phisher can access the victims' bank accounts or assume control of their social network.
Fiscal fraud	By targeting official online payment channels, cyber attackers can hamper processes such as tax collection or make fraudulent claims for benefits.[10]
State cyber attacks	Experts believe that some government agencies may also be using cyber attacks as a new means of warfare. One such attack occurred in 2010, when a computer virus called Stuxnet was used to carry out an invisible attack on Iran's secret nuclear program. The virus was aimed at disabling Iran's uranium enrichment centrifuges.[11]
Carders	Stealing bank or credit card details is another major cyber crime. Duplicate cards are then used to withdraw cash at ATMs or in shops.

Increasing cyber crime

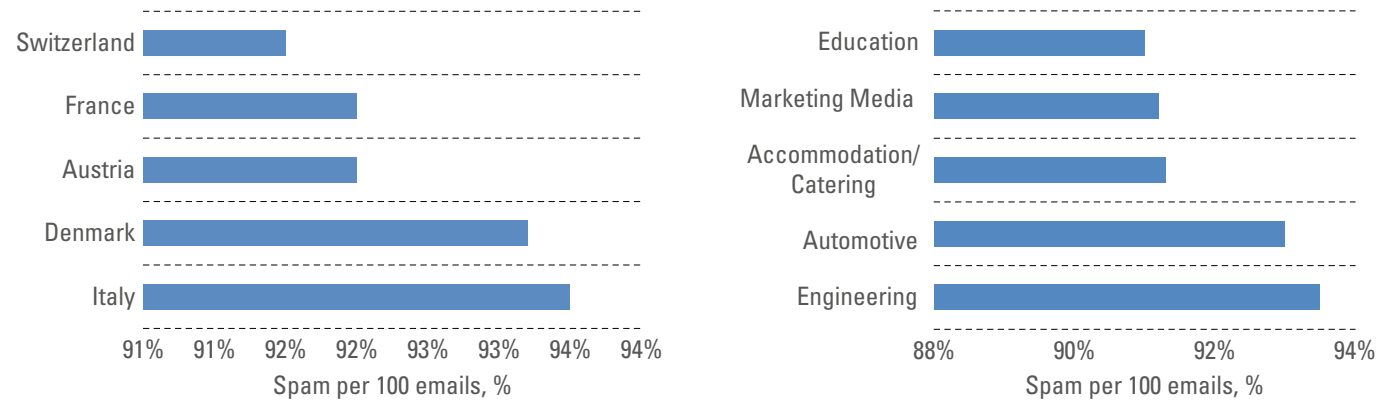
Over the past few years, the global cyber crime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security. Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent. These attacks, which were rarely malicious, have gradually evolved into cyber crime syndicates siphoning off money through illegal cyber channels. By 2010, however, politically motivated cyber crime had penetrated global cyberspace.[12] In fact, weaponry and command and control systems have also transitioned into the cyberspace to deploy and execute espionage and sabotage, as seen in the example of digital espionage attacks on computer networks at Lockheed Martin and NASA.[13]

> In 2010, the number of malicious software programs specifically targeting mobile devices grew by 46 percent.

- In 2010, the global spam rate increased 1.4 percent year-on-year (y-o-y), to 89.1 percent, most of which involved botnets, according to a Symantec report.[14]
- In 2010, the average rate of malware in email traffic was 1 in 284.2 emails, almost the same as that in 2009. However, the average rate of emails blocked as phishing attacks improved from 1 in 325.2 in 2009 to 1 in 444.5 in 2010.[15]
- The average number of blocked malicious websites rose from 2,465 per day in 2009 to 3,188 in 2010.[16]
- In 2010, a major attack came from a complicated computer worm Stuxnet. The worm — which infected a large number of industrial controls worldwide — was able to give false machinery instructions, subsequently leading to nuclear malfunctions and break-down operations at gas pipelines. The worm's target location was believed to be Iran, but it also affected Indonesia, India and Pakistan.[17]

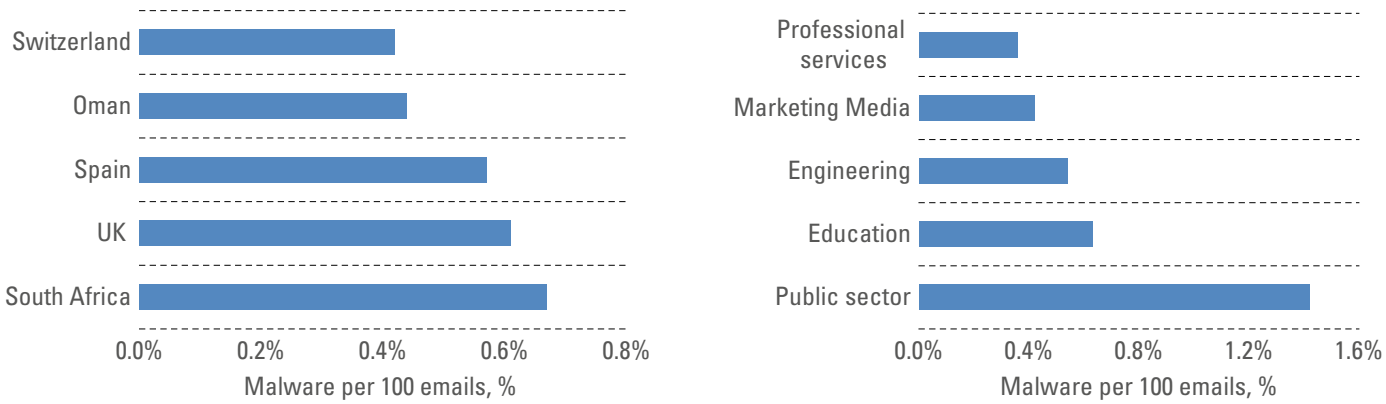
Cyber criminals are now moving beyond computers, and attacking mobile handheld devices, such as smartphones and tablet personal computers (PCs). In 2010, the number of malicious software programs specifically targeting mobile devices, rose 46 percent, according to information technology (IT) security group McAfee. Cyber criminals are taking

Figure 1: Global email spam rate (as detected by MessageLabs Services, Symantec), top 5 targeted geographies and sectors, 2010



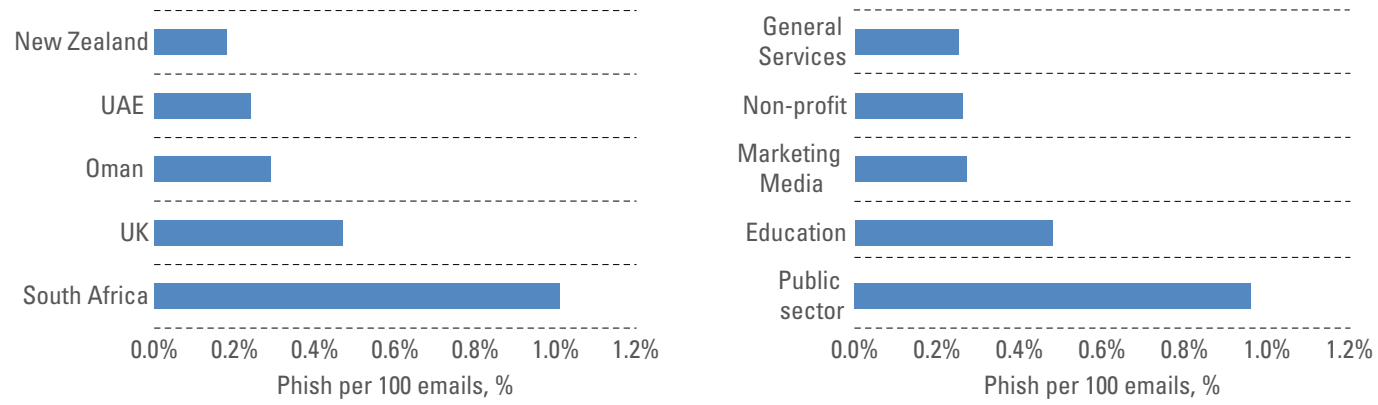
Source: MessageLabs Intelligence: 2010 Annual Security Report, Symantec

Figure 2: Global email malware rate (as detected by MessageLabs Services, Symantec), top 5 targeted geographies and sectors, 2010



Source: MessageLabs Intelligence: 2010 Annual Security Report, Symantec

Figure 3: Global phishing rate (as detected by MessageLabs Services, Symantec), top 5 targeted geographies and sectors, 2010

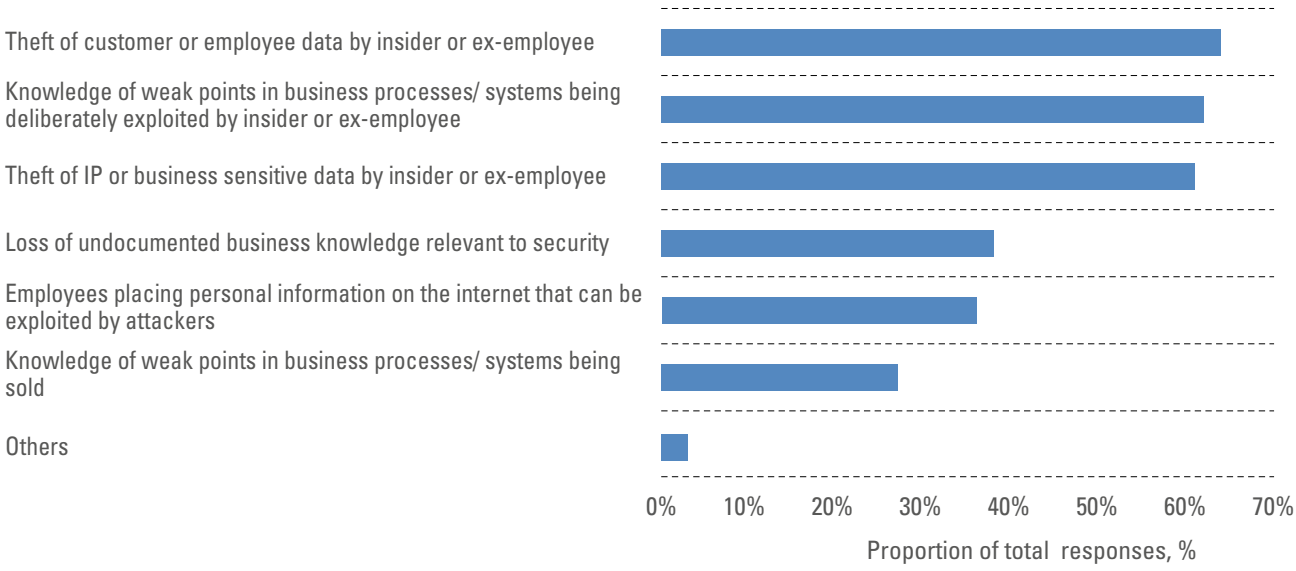


Source: MessageLabs Intelligence: 2010 Annual Security Report, Symantec

advantage of the increasing popularity of mobile phone applications and games by embedding malware into them.[18]

In addition, information systems face risks resulting from human error or dishonesty. With incidents such as the hacking of Google and WikiLeaks disclosures, it has become critical to acknowledge the risks to information systems due to human behavior. According to a 2009 e-crime survey by KPMG, the major e-crime risks identified by the respondents were related to insiders or former employees, as shown in Figure 4. These sentiments were echoed by Eric Bonabeau, founder and Chairman of Icosystem Corporation, who said, "Obviously, it is essential to continue to improve the technical aspects of cybersecurity and significant investment needs to be made to ensure continuous progress — and to keep up with increasingly sophisticated enemies. But at the same time, human behavior is almost always the weakest link in security."[19]

Figure 4: Which internal e-Crime risks are of most concern in the current economic climate?



Source: E-Crime Survey 2009, KPMG

Implications of rising cyber crime

> In 2009, the cost of information lost to cyber crime nearly doubled, from US$265 million in 2008 to US$560 million.

Every day, nearly 150,000 viruses and other malicious codes circulate through cyberspace, affecting 148,000 computers in corporate and government offices.[20] In the US over the course of one year in 2009, the amount of information lost to cyber crime nearly doubled, from US$265 million in 2008 to US$560 million, according to a report by the Internet Crime Complaint Center (IC3), which is supported by the US Federal Bureau of Investigation. Most losses of this nature have resulted from cyber scams, where criminals posed as government agents, collecting information, while others include non-delivery of merchandise or payment.[21] Moreover, the international nature of cyber crime results in the involvement of not only the target region, but also other countries or regions from where the attacks originate. Consequently, cyber crime requires highly responsive and internationally coordinated control measures, making investigation and reporting of such crimes resource-intensive.[22]

> "Cybercrime is emerging as a very concrete threat. ...Considering the anonymity of cyberspace, it may in fact be one of the most dangerous criminal threats we will ever face."
>
> *– Ronald K. Noble, Secretary General, Interpol*

Countries face cost escalation

As corporations and government offices are increasingly becoming the target of cyber attacks, the costs to maintain, protect and restore cyber infrastructure have increased rapidly.[24] In the UK, the annual cost resulting from cyber crime is estimated at GBP27 billion (US$43 billion). A major portion of that is the result of intellectual property (IP) theft, which is expected to account for an annual total of GBP9.2 billion (US$14 billion), while espionage activities are expected to cost more than GBP7 billion (US$11 billion).[25] In Germany, phishing activity is estimated to have increased 70 percent year-over-year in 2010, resulting in a loss of EUR17 million (US$22 million), according to a joint report by the German information technology trade group Bitkom and the German Federal Criminal Police Office.[26]

According to the report 'The Cost of CyberCrime' released by the UK Cabinet Office, the following are the major areas that can affect a government organization's cost structure:[27]

- Costs in anticipation of cyber crime: Security measures, such as antiviral software installation, cost of insurance and IT security standards maintenance.
- Costs as a consequence of cyber crime: Monetary losses to organizations, such as gaps in business continuity and losses due to IP theft.
- Costs in response to cyber crime: Paying regulatory fines and compensations to victims of identity theft, and cost associated with investigation of the crime.
- Indirect costs associated with cyber crime: Costs resulting from reputational damage to organizations and loss of confidence in cyber transactions.

In efforts to combat digital crime, government spending on cyber security has increased significantly. In February 2011, the UK government allocated GBP63 million (US$100 million) to build upon the existing expertise within the UK Serious Organised Crime Agency (SOCA) and the Met Police Central e-Crime Unit.[35] Similarly, for 2012, the US Pentagon increased its budget to protect military networks, to US$3.2 billion.[36]

Table 2: Major attacks that inflicted monetary damages

Type of attack	Time	Details	Estimated damages
Stuxnet worm	2010–11	Stuxnet was launched with the intention of damaging utilities companies and nuclear facilities in Iran and other countries. The program reportedly destroyed a fifth of Iran's nuclear centrifuges.[28]	Unknown
Night Dragon	2009–11	Night Dragon is a major cyber espionage program that is currently affecting many Western companies. According to McAfee, hackers targeted five major multinational companies (mostly in the oil and gas sector), stealing sensitive data on proprietary information about oil and gas field operations, project financing and bidding documents.	Not available
Operation Aurora	2009–11	In 2010, Google reported IP theft and illegal access to the Gmail accounts of human rights activists. The attacks are being investigated under the code name 'Operation Aurora'.[29]	Not available
Zeus botnet	2007–11	This botnet steals personal information by infecting computers and capturing data entered into internet banking sites, including passwords. Currently, the program has evolved more, and can produce 700 variants every day, including mobile capabilities.[30]	In July 2010, major UK banks reported being affected by Zeus. Within a month, it stole GBP700,000 (US$1.1 million) from 3,000 online customers.[31]
Conficker malware[32]	2007	This worm was designed to download and install malware from sites controlled by the virus writers. Thereafter, these criminals could easily access the PC users' personal information and even their PCs.	US$9.1 billion
MyDoom's mass infection[33]	2004	This worm was designed to infect computers and send spam emails. As mass volumes of spam mails were sent, internet access around the world slowed down 10 percent. The worm also reduced access to some websites by 50 percent, resulting in losses due to low productivity and reduced online sales.	US$38 billion
'I Love You' worm[34]	2000	This spam email had a subject line —'I love you'— which led many users to open it, most of whom downloaded the attached 'love letter' file. The worm then affected their computers, costing companies and government agencies approximately US$15 billion to repair the damage.	US$15 billion

> "Cyber-espionage is the biggest intelligence disaster since the loss of the nuclear secrets (in the late 1940s)."
>
> *– Jim Lewis, Director, Centre for Strategic and International Studies*[37]

> "To address the severe global problem of cyber crime, governments and legal authorities are faced with a difficult task. Not only must they identify what actions to take post attack, they must also think one step ahead, focusing on preventing the threat's recurrence."
>
> *– Rosemary Scully, Global Head of Justice and Security, KPMG*

Cyber war and espionage against governments is on the rise

Over the last few years, cyber attacks have evolved in utilizing online weapons affecting government entities. Richard Clarke, a former US White House staffer in charge of counter-terrorism and cyber security, notes that a full-scale cyber attack on a country's important infrastructure, such as military email systems, air traffic control systems, financial markets and utilities could have an unprecedented long-term effect. Experts believe that the world has already witnessed glimpses of cyber war, with cyber espionage hackers stealing important state information or crippling government offices.[38]

The **US** defence system has been targeted on several occasions.

- In March 2011, US officials announced that they were investigating plans by members of the hacking group 'Anonymous' to hack into the Marine Corps base in Quantico, VA. The group is a major protestor of the US government's actions against whistleblower WikiLeaks. The reason the hacking group is allegedly targeting the base is that one of the alleged informers to WikiLeaks is incarcerated there.[39]
- In 2009, computer hackers broke into the Pentagon's US$300 billion Joint Strike Fighter project, F-35 Lightning II. The F-35 program is the costliest weapons program ever. As hackers carefully encrypted the stolen data, investigators were unable to determine the amount or nature of the lost data.[40]
- In 2008, the US military's classified computer network was hacked by an unidentified intelligence agency, which inserted a malicious code into the system through a flash drive. As a result of the incident, the Pentagon banned the use of USB drives as of November 2008.[41]
- In June 2007, the Pentagon was forced to disable up to 1,500 computers, as hackers breached an email system at the Office of the Secretary of Defence.[42]

Canada has also been a victim of a cyber attack.

- In January 2011, hackers infected computers in two Canadian government departments, leaving many officials without internet access for nearly two months.[43]

Estonia and **Georgia** witnessed the Web War I.

- In 2007, Estonia became the target of a DoS attack that came to be known as 'Web War I' (or WWI), which affected the country's government, media and banking web servers. In 2008–09, a similar cyber attack took place in Georgia during its war with Russia. This led President Mikheil Saakashvili to move the website to Tulip Systems, a US-based server, which was capable of fighting off the attack more effectively.[44, 45]

Global summits are prime targets for hackers.

- In March 2011, the computer network at the EU headquarters was targeted by hackers, prior to an EU leaders' summit on economic reforms and current affairs.[46]
- In December 2010, computer hackers broke into computers at the French Finance Ministry and stole sensitive information related to the G20 Summit that was held in France in February 2011. The criminals took control of nearly 150 computers at the French Finance Ministry, and accessed many documents that had sensitive information on the G20 summit.[47]

Impact of cyber crime on justice systems of a country

In addition to affecting a country's defence system, cyber crime also puts a significant burden on its justice systems. In the US, in 2010, the Internet Crime Complaint Center (IC3) received 303,809 complaints related to cyber crime. This was slightly down from the 336,655 in 2009.

The largest number of complaints was from people who had been deceived by criminals posing as buyers and sellers. In February 2010, a Romanian national, Adrian Ghighina, pleaded guilty to his role in a scam that took in US$2.7 million by deceiving eBay, craigslist and AutoTrader.com users into paying for vehicles that were never delivered.[48] In March 2007, five Eastern Europeans were imprisoned in the UK for credit card fraud. They stole an estimated GBP1.7 million (US$2.8 million).[49]

Espionage activities affect private companies

In addition to government entities, many companies in the energy, defense and pharmaceutical sectors are also becoming the targets of espionage and IP theft. According to the UK Cyber Cabinet Office, industrial cyber crime, including firms spying on each other, costs around GBP7.6 billion (US$12.4 billion).[50]

> In the US in 2010, the Internet Crime Complaint Center (IC3) received 303,809 complaints related to cyber crime.

- An unspecified FTSE 100 (Financial Times Stock Exchange Index) company, had to shut down its entire email system for two weeks, after it became the target of a cyber attack.[51]
- IP theft costs US organizations nearly US$200–250 billion annually, according to estimates from the US Commerce Department.[52]
- According to a 2009 e-Crime Survey by KPMG, results from 45 percent of the respondents, indicated an increase in phishing activities.[53]

What are governments doing to fight cyber battle?

> In October 2010, the UK government commited to providing GBP650 million (US$1 billion) to cyber security initiatives.

According to the US Defense Secretary Robert Gates, cyberspace is the new domain in which war will be fought, after land, sea, air and space.[54] The US government has been focusing on protecting its digital infrastructure, declaring it a 'strategic national asset.' Similarly, Iran, Israel, North Korea, Russia and many other countries are now creating and training 'cyber armies'. Such increased vigilance is gaining attention, as both governments and corporate entities have become prime targets of cyber attacks.[55]

Countries cracking down on cyber crime

US is facilitating global cyber security

- In January 2011, US Senators Joseph Lieberman and Susan Collins re-introduced a bill — the Cybersecurity and Internet Freedom Act of 2011 — granting President Barack Obama the authority to shut down the internet in the country in the event of a cyber attack. However, the bill is still under debate, and has been opposed by many organizations that believe it may give the government more power and control over the internet.[56, 57] Privacy experts such as Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, believe that such a bill could obstruct communication and economic activities.[58]
- In January 2011, the US Department of Commerce announced that it is planning to launch an office — the National Strategy for Trusted Identities in Cyberspace (NSTIC) — to promote online trusted identity technologies. The NSTIC aims to promote a platform where internet users will receive IDs, thereby increasing trust among users.[59]
- The US Federal Bureau of Investigation (FBI) has established a separate division to address cyber crime in a coordinated manner.[60] In October 2010, the FBI arrested more than 90 people, who were believed to be engaged in an international crime syndicate that hacked into US computer networks to steal US$70 million. Hackers used spam email to target the computers of small businesses and individual users. By gaining access to users' passwords and bank account details, the hackers were able to transfer money from those accounts.[61]

> In January 2011, Iran officially launched its cyber police unit to ramp up its fight against cyber crime.

UK is investing to improve its defense tactics against cyber crime

- The UK considers cyber crime to be a tier 1 threat, equating it to international terrorism and major incidents.[62] In 2008, the Police Central e-Crime Unit (PCeU) was set up to fight national cyber crime. The PCeU collaborates with law enforcement agencies and private industries.[63]

- In October 2010, the UK government commited to providing GBP650 million (US$1 billion) to cyber security initiatives.[64] By February 2011, GBP63 million (US$100 million) had been allocated for cyber security. According to a UK government spokesman, "The government is determined to build an effective law enforcement response to the cyber crime threat, building upon the existing expertise within SOCA (national police unit responsible for pro-active operations against serious and organized crime) and the Met Police Central e-Crime Unit."[65]
- Apart from increasing investments, the UK also plans to coordinate with Poland on information security policy while planning for the Euro2012 football championships and the London 2012 Olympics.[66]

China is fighting cyber crime with the international support

- Although China has been regarded as the largest source of targeted hacking attacks, the country is also on the receiving end of attacks. In 2009, nearly 200 Chinese government websites were attacked or infiltrated daily.[67]
- In 2009, China incorporated computer crimes into its criminal law legislation.[68]
- The country is collaborating with the UN, Association of Southeast Asian Nations (ASEAN) and other international communities and governments in efforts to fight cyber crime.
  - In 2003, China signed the ASEAN-China Coordination Framework for Network and Information Security Emergency Responses and an agreement among the governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security with the ASEAN and SCO member states, respectively.[69, 70]
  - The US has been supporting the Chinese government in its fight against cyber crime. Over 2009–10, the US provided assistance to China in 13 major cases of internet crime.[71]
- In an effort to protect confidential information, by May 2010, China had tightened its Guarding State Secrets law, by holding internet and mobile phone operators responsible for customers who try to leak confidential information.[72]

Iran is launching cyber police unit

- In January 2011, Iran officially launched its cyber police unit to ramp up its fight against cyber crime. The designated web watchdog team will be responsible for targeting specific networking websites that engage in espionage and incite riots.[73]
- By the end of 2011, nearly all police stations in Iran will have their own cyber police unit.[74]

Indian government is setting up IT institute

- In January 2011, the Indian government announced that it plans to set up an institute dedicated to training professionals and developing technologies to tackle cyber crime. The institute will be a public-private partnership initiative, with a total cost of INR1 billion (US$21 million).[75]
- In November 2010, India's Central Bureau of Investigation (CBI) signed an agreement with industry body Nasscom to share expertise on ways to counter cyber attacks.[76]
- In July 2010, the Indian government proposed an initiative to develop a unit that will include a group of hackers acting as a specialized team as counter offence to hacking activities from foreign countries. The National Technical Research Organisation (NTRO), along with the Defence Intelligence Agency (DIA), was delegated to create this capability.[77]

International organizations zero in on cyber security

Europol enforces EU cyber security initiatives

- In June 2010, Europol (the EU's law enforcement agency) created the European Union Cyber crime Task Force.[78] The task force includes an expert group of representatives from Europol, Eurojust (the EU judicial cooperation body) and the European Commission.[79]
- Europol provides the EU members with investigative and analytical support on cyber crime, and facilitates cross-border cooperation and information exchange.[80]

NATO alliance provides platform for coordinated initiative[81]

- At the North Atlantic Treaty Organization (NATO) summit in November 2010, the EU, NATO and the US, approved plans for a coordinated approach to tackle cyber crime in member states. Under the approval, by 2013, an EU cyber crime center will be established to coordinate cooperation between member states. Also by that time, a European information sharing and alert system will facilitate communication between rapid response teams and law enforcement authorities.
- By 2012, the European Commission is expected to create a network of Computer Emergency Response Teams (CERTs) — that can react in case of computer-related emergencies, such as cyber attacks — with a CERT center in each EU country.

Challenges faced by governments

Although governments are actively focused on fighting and preventing cyber criminals from damaging infrastructure, the very nature of cyberspace poses a number of challenges to the implementation of cyber regulations in any country. Within cyberspace it is often difficult to determine political borders and culprits. Furthermore, the cyber criminal community and their techniques are continously evolving, making it more challenging for governments and companies to keep up with ever-changing techniques.

Tracking the origin of crime

According to Rob Wainwright, Director of Europol, criminal investigations of cyber crimes are complex, as the criminal activity itself is borderless by nature.[82] Tracing cyber criminals poses a challenge. While many experts speculate that the cyber attacks on Estonia and Georgia, for instance, were directed by the Russian cyber agencies, some of the attacks have been traced to the computers originating in Western countries.[83]

Growth of the underground cyber crime economy

A major threat that may hamper the fight against cyber crime is the growth of an underground economy, which for many cyber criminals can be a lucrative venture. The underground economy attracts many digital experts and talented individuals with a specialty around cyber initiative.[84] In the cyber underworld, the hackers and organized crime rings operate by selling confidential stolen intelligence. Research shows that criminals are trading bank account information for US$10–125, credit card data for up to US$30 per card, and email account data for up to US$12.[85] Often, the aquired data is used in illegal online purchases and in exchange for other monetary transactions. The untraceability of the origin of these transactions poses a major challenge to government agencies in their efforts to fight crimes of this nature.[86]

Shortage of skilled cyber crime fighters

Implementing cyber security measures requires skilled manpower. However, most countries face a shortage of skilled people to counter such cyber attacks. According to Ronald Noble, Head of Interpol, "An effective cyber attack does not require an army; it takes just one individual. However, there is a severe shortage of skills and expertise to fight this type of crime; not only at Interpol, but in law enforcement everywhere."[87]

Moreover, most trained or skilled people are recruited by the private sector, as it offers higher financial rewards. In the UK, the PCeU has experienced this shortage first hand, with only 40 core team members.[88] Similarly, in Australia, the majority of the cyber crime incidents, particularly minor incidents, remain unsolved or are not investigated due to the lack of eForensic skills and expertise.[89]

> Criminal investigations of cyber crimes are complex, as the criminal activity itself is borderless by nature, according to Rob Wainwright, Director of Europol.

> Collaboration between governments is imperative in order to fight cross-border e-Crime.

> China reported that nearly US$19 billion was spent on pirated software, in 2009.

Widespread use of pirated software

One of the major challenges to preventing cyber crime is the prevalence of software piracy, as pirated software is more prone to attacks by viruses, malware and trojans. Experts believe that the rapid growth of consumer PC markets in emerging countries — such as India, Brazil and China — has contributed largely to the rising piracy rates.[90]

The pirated software can include not only games, movies, office applications and operating systems, but also security software. Often, users prefer to obtain a pirated security software, rather than purchase and upgrade legal version, therefore increasing the vulnerability of their systems to cyber attacks.[91] For instance, one of the reasons for the spread of the Conficker virus in 2008 was the lack of automatic security updates for unlicensed software.[92] The issue becomes more significant for those countries where pirated software is a common occurance.

- China, which is one of the largest such markets, reported that nearly US$19 billion was spent on pirated software in 2009.[93]
- In India, the unlicensed software market value stands at nearly US$2 billion.[94]
- Ensuring cyber security is also a major challenge for Gulf Cooperation Council (GCC) countries, where 50 percent of software is pirated.[95]

Forecast

Experts believe that to fight the borderless and continuously evolving cyber crime, global leaders must collaborate in joint initiatives. Nigel Inkster, an expert on cyber threats at the International Institute for Strategic Studies, stated, "Thus far, the discussion on how to set international standards on cyber has been very low profile and largely confined to the margins of the UN General Assembly." However, to overcome significant diplomatic hurdles, a concerted effort on the part of governments must be in place.[96] In April 2010, the UN rejected a treaty on global cyber crime, due to disagreements over the national sovereignty issues and concerns for human rights. Many countries have expressed a concern over the new cyber laws. Russia, as one of the examples, has refused to endorse the 'Budapest Convention on Cybercrime,' which allows police and other legal entities to cross national boundaries without the consent of local authorities, in order to access computer servers.[97]

However, country officials in most developed nations do agree on the establishment of policies to protect cyberspace against criminals.[98] Experts believe that developed countries such as the US should encourage other countries to introduce policies against cyber attacks, in the similar fashion they do for nuclear weapons, missile defense and space.[99] "The US has to frame a much clearer strategy with regard to cyber (warfare)," said Greg Austin, Vice President of Program Development and Rapid Response at the EastWest Institute.[100] The US supports an International Telecommunication Union plan, which obligates the country of origin of Cyber crime acts to conduct investigation. The US also supports a Russian initiative that has called for a UN panel to work on cyber-arm limitations. However, experts believe that the implementation of such a coordinated initiative might take a few more years.[101]

Apart from bilateral and multi-lateral initiatives between governments, much can be achieved by cooperating with the private companies that own and control the majority of the cyberspace network. Network owners or internet-service providers can take more responsibility to help identify cyber attacks and attackers on user computers, and take the necessary steps to counter such attacks. Experts believe that while such preventive measures may not completely eliminate cyber espionage, it can certainly make cyberspace a much safer place.[102]

> Thus far, the discussion on how to set international standards on cyber has been very low profile and largely confined to the margins of the UN General Assembly.

> Engaging private players in the fight against private companies could be helpful for governments to tackle this situation.

Further Information

Visit kpmg.com for the following related publications

- *e-Crime Survey 2009 KPMG International*

How KPMG firms can help

Assessing Vulnerabilities and Providing Protection

KPMG firms' Information Protection and Business Resilience teams deliver a broad range of services to identify and assess an organisation's cyber crime vulnerabilities. Services include security testing to assess technical controls around infrastructure, systems and applications; identity & access management to improve authentication, authorization and access management; and information governance to protect information assets throughout their lifecycle.

Combating fraud

Fraud is one of the most difficult risks to detect but it is an ever-evolving and costly threat to the finances and reputations of many organizations. Operating in both developed and emerging markets, KPMG firms' forensic specialists provide robust and practical advice on reducing reputational risk and commercial losses.

Managing financial risk

With 1,600 financial risk management practitioners around the world, KPMG's experience spans industries and geographies. We help our firms' clients create frameworks to efficiently control business and financial risk. This process involves not only identifying, assessing, managing, reporting and mitigating risks, but also by providing guidance regarding the nature of risks that are within their reach to address to provide impetus to their business growth.

Key contacts

John Herhalt
Global Head of Government
KPMG in Canada
Tel.+1 416 777 8778
jheralt@kpmg.ca

Rosemary Scully
Global Head of Justice and Security
KPMG in UK
Tel.+44 207 311 1516
Rosemary.Scully@kpmg.co.uk

Organizations Mentioned in this Issue

Sources

1 *The cost of cybercrime,* Detica, February 2011

2 *It is time for countries to start talking about arms control on the internet,* Economist, July 1, 2010

3 *The worldwide crime web,* BBC News

4 *MessageLabs Intelligence: 2010 Annual Security Report,* Symantec

5 *Cyber attacks: from Facebook to nuclear weapons,* The Telegraph, February 4, 2011

6 *A Good Decade for Cybercrime,* McAfee, 2010

7 Accessed from Spamhaus on March 10, 2011

8 Accessed from PCMeg.com on March 10, 2011

9 *The cost of cybercrime,* Detica, February 2011

10 *The cost of cybercrime,* Detica, February 2011

11 *Cyber attacks: from Facebook to nuclear weapons,* The Telegraph, February 4, 2011

12 *National insecurity,* InformationAge, January 26, 2011

13 *Stuxnet was about what happened next,* FT.com, February 16, 2011

14 *MessageLabs Intelligence: 2010 Annual Security Report,* Symantec

15 *MessageLabs Intelligence: 2010 Annual Security Report,* Symantec

16 *MessageLabs Intelligence: 2010 Annual Security Report,* Symantec

17 *Stuxnet worm causes worldwide alarm,* FT.com, September 23, 2010

18 *Threat of mobile cybercrime on the increase,* FT.com, February 8, 2011

19 *Human Factor Missing in Cybersecurity?,* The New New Internet, April 16, 2011

20 *Cybercrime presents a major challenge for law enforcement,* EUROPOL, January 3, 2011

21 *U.S. cybercrime losses double,* HSNW, March 16, 2010

22 *Internet Facilitated Organised Crime,* iOCTA, January 2011

23 *Cybercrime is world's most dangerous criminal threat,* Physorg, September 17, 2010

24 *The cost of cybercrime,* Detica, February 2011

25 *The cost of cybercrime,* Detica, February 2011

26 *Cybercrime in Germany on the rise,* DW World, September 7, 2010

27 *The cost of cybercrime,* Cabinet Office (UK), February 2011

28 *Israeli Test on Worm Called Crucial in Iran Nuclear Delay,* NYTimes, January 15, 2011

29 *Google Hack Attack Was Ultra Sophisticated, New Details Show,* Wired, January 14, 2010

30 *A Good Decade for Cybercrime,* McAfee, 2010

31 *Playing with Firewalls,* WSJ, October 5, 2010

32 *A Good Decade for Cybercrime,* McAfee, 2010

33 *A Good Decade for Cybercrime,* McAfee, 2010

34 *A Good Decade for Cybercrime,* McAfee, 2010

35 *£63m to tackle UK cybercrime,* Public Services, February 15, 2011

36 *Pentagon seeks $3.2 billion for revised cyber budget,* Nextgov, March 24, 2011

Sources

37 *War in the fifth domain,* Economist, July 1, 2010

38 *War in the fifth domain,* Economist, July 1, 2010

39 *US probes Anonymous plans for attack on marines,* FT.com, March 8, 2011

40 *Computer Spies Breach Fighter-Jet Project,* WSJ, April 21, 2009

41 *Pentagon Official Says Flash Drive Used in Classified Cyberattack,* AoL News, August 25, 2010

42 *Pentagon Target of Cyber Attack,* Betanews, June 21, 2007

43 *Canada Hit by Cyberattack,* NYTimes, February 17, 2011

44 *War in the fifth domain,* Economist, July 1, 2010

45 *Under Cyberattack, Georgia Finds 'Bullet-Proof' Hosting With Google And Elsewhere,* InformationWeek, August 12, 2008

46 *EU Headquarters Under Cyber Attack Before EU Leaders' Meeting,* Bloomberg, March 24, 2011

47 *Cyber attackers target G20 documents,* FT.com, March 7, 2011

48 *US cybercrime complaints fell 10% in 2010,* Computerworld Inc, February 24, 2011

49 *The Cybercrime Arms Race, SecureList,* September 17, 2008

50 *Cyber crime 'costs UK £27bn a year',* Guardian News and Media Limited, February 2011

51 *Cyber thieves get personal,* FT.com, January 26, 2011

52 *Computer Crime & Intellectual Property Section,* Accessed from Justice.gov as on May 3, 2011

53 *E-Crime Survey 2009,* KPMG

54 *Who controls the internet?,* FT.com, October 8, 2010

55 *War in the fifth domain,* Economist, July 1, 2010

56 *Internet 'kill switch' bill reintroduced as Egypt remains dark,* Network World, January 31, 2011

57 *Will the U.S. get an Internet "kill switch"?,* Technology Review, March 4, 2011

58 *'Kill Switch' Internet bill alarms privacy experts,* USAToday, February 15, 2011

59 *White House Officials Push Online Trusted IDs,* PCWorld, January 8, 2011

60 *Computer Intrusions,* The Federal Bureau of Investigation

61 *More than 100 arrests, as FBI uncovers cybercrime ring,* BBC, October 2010

62 *UK cyber security plans 'essential for strong defence',* BBC, October 18, 2010

63 *Interview: Head of the PCeU, Charlie McMurdie,* Computing.co.uk, November 11, 2010

64 *Cameron sets aside £650m to fight cybercrime,* which.uk, October 20, 2010

65 *£63m to tackle UK cybercrime,* Public Services, February 15, 2011

66 *Cybercrime policing to get £63m boost,* ZDNet, February 16, 2011

67 *Internet policing hinges on transnational cybercrime,* China.org, November 10, 2010

68 *Internet policing hinges on transnational cybercrime,* China.org, November 10, 2010

Sources

69 *China's Cybersecurity and Pre-emptive Cyber War,* EastWest Institute, March 14, 2011

70 *Full Text: The Internet in China,* Xinhuanet, June 8, 2010

71 *Internet policing hinges on transnational cybercrime,* China.org, November 10, 2010

72 *China addresses 'severe cyber security threats',* China Daily, May 6, 2010

73 *Iran launches cybercrime unit: police,* AFP, January 23, 2011

74 *Iran launches cybercrime unit: police,* AFP, January 23, 2011

75 *Govt plans to set up IT Institute to tackle cybercrime,* Silicon India, February 16, 2011

76 *CBI Inks Pact With Nasscom To Fight Cyber Crime,* Businessworld, November 22, 2010

77 *Spy Game: India readies cyber army to hack into hostile nations' computer systems,* Economic Times, August 6, 2010

78 *European Union Cybercrime Task Force,* Europol

79 *Cybercrime presents a major challenge for law enforcement,* Europol

80 *Cybercrime presents a major challenge for law enforcement,* Europol

81 *EU and US join NATO cyber security pact,* Computerworld, November 23, 2010

82 *Europol to reveal cybercrime risk level,* Computerworld, January 6, 2011

83 *War in the fifth domain,* Economist, July 1, 2010

84 *The cost of cybercrime,* Detica, February 2011

85 *Cybercrime as a business: The digital underground economy,* Europol, January 6, 2011

86 *Cybercrime As A Business: The Digital Underground Economy,* Voxy, January 7, 2011

87 *Interpol Boss Warns Of Cybercrime Skills Shortage,* Dot ie, November 15, 2010

88 *Cyber skills a top challenge, says UK police cybercrime unit,* Computerweekly, November 11, 2010

89 *Australian cybercrime investigation skills lacking says Swinburne professor,* TechWorld, November 5, 2010

90 *'Software piracy benefits only criminals',* CIOL, June 15, 2010

91 *Cybercrime Challenges in the GCC,* ITP.net, May 6, 2010

92 *New study reveals extent of PC software piracy worldwide,* BSA, May 12, 2009

93 *China says software piracy declines -- to 19 billion dollars,* AFP, May 10, 2010

94 *'Software piracy benefits only criminals',* CIOL, June 15, 2010

95 *Cybercrime Challenges in the GCC,* ITP.net, May 6, 2010

96 *UK seeks global accord on cyber threat,* FT.com, February 3, 2011

97 *Global cybercrime treaty rejected at U.N.,* SC Magazine, April 23, 2010

98 *Global cybercrime treaty rejected at U.N.,* SC Magazine, April 23, 2010

99 *Cyberwar,* Economist, July 1, 2010

100 *Rules of engagement for cyberwars see slow progress,* FT.com, December 28, 2010

101 *Rules of engagement for cyberwars see slow progress,* FT.com, December 28, 2010

102 *Cyberwar,* Economist, July 1, 2010

Notes

Contact us

John Herhalt
Global Head of Government
KPMG in Canada
T: +1 416 777 8778
E: jheralt@kpmg.ca

Rosemary Scully
Global Head of Justice and Security
KPMG in UK
T: +44 2073111516
E: Rosemary.Scully@kpmg.co.uk

Designed and produced by Evalueserve

Contact: Vipin Kumar
Head of Global Markets Research
KPMG in India
Tel.+91 124 612 9321

Publication name: Issues Monitor
Publication number: 11 - 008
Publication date: July 2011