CCC News
Control Computer Crimes
Issue 0002 30 June 2009

UK confesses cyber attack capabilities Page1

Can you trust your vendor? Page 16

Cyber Security Series
Backup your files Page 28

Message from Editor

Welcome to the second issue of CCCNews Magazine.

More than 100,000 downloads have been recorded, of our first issue, from our website www.cccnews.in. This is highly encouraging and professionally satisfying result of presenting a new publication, i.e. CCCNews Magazine.

I thank all the constituents, who have taken interest in downloading and reading the first issue of CCCNews Magazine. I further request the readers to circulate the publication weblink to their friend and colleagues, so that more and more people can take advantage of the CCCNews magazine.

I am happy to present you this second issue of the CCCNews Magazine.

Cyber space has been experiencing extra ordinary turbulence. Iran has accused USA based entities like CNN that they are training hackers to attack Iran's cyber space. Networking portals like 'Twitter' is being used for DDos Attacks on Iran government websites. If it is true, this is really dangerous game. This is like 'Riding a Tiger'. And those, who rides a tiger, tiger finally rides them. Once the weapon level usage of specific web-based portals or sites or tools are in public domain, these will become weapons of mass destruction (WMDs), even against those, who have used it first.

On the other hand, USA has establishing a cyber security command that will defend military networks against computer attacks and develop offensive cyber-weapons, but he also directed that the structure be ready to help safeguard civilian systems. Similarly, UK government plans to form a cybersecurity agency, with functions including cyberattack capability. This agency will work on the line of USA agency.

Similarly, the European Commission has proposed setting up an agency to manage the region's large IT systems containing passport, visa and fingerprint information.

On the other side of the globe, China has planned to compulsory install an official filtering software, called *'Green Dam Youth Escort'* on all computers sold in China effective 01 July 2009. The software provided the powers to government to block all porn and obscene material/site apart from other political uncomfortable site. The software has been found with many holes / bugs, which can be exploited by any Botnet. An American company even accused Chinese of stealing their software. US protested this Chinese move to protect their PC industry. Chinese have postponed the launch of the software till all bugs / vulnerabilities are addressed and made the use of the software optional. Apart from technological, this is psychological and political war.

Phishing and Scam artists are getting more smarter. These people have wasted no time in exploiting the death of Michael Jackson and Farrah Fawcett for email harvesting and banking Trojan campaigns. More are expected in future.

Now RSS feed are under hacker attack. According to a report there has been a rise in the number of RSS feeds being hacked into lately. Similarly, in another report, it is reported vendors secretly left undocumented privileged administrator accounts in new network routers belonging to two telecoms service providers as a backdoor traps.

All the above is the tip-of-the-iceberg glimpses of - what is happening in cyber crime world. I can not put all, that has happened in last fortnight in this message. But, the objective is that we all should be aware of these threats and risks. These threats and risks affect all computer users. My purpose of highlighting these incidents and publishing CCCNews is that unless we know the threat, we can not plan for threat mitigation. 2000 years back, Acharya Chanayka said that "Unless you know the Enemy, you can not fight the battle". And we are talking of winning the war.

Rakesh Goyal
Editor

Message from Secretary-General

It was a journey initiated in June 2005, when we had our First CRPCC Newsletter, which was done with a motto of making aware of the latest issues related to the Information Security issues on a single platform. Four years down the line, we have published about 700+ issues and read by over 85,000 subscribers.

This new offering of ours - CCCNews Magazine is the result of our experience with our four years of intense publication of CRPCC Newsletter.

I am sure that you all may have liked our inaugural issue, published on 15th June 2009. I hope this magazine will enhance communication among the important groups making up our community — IT users, IT Security professionals, alumni and friends, students, researchers, faculty, and all other stake-holders. We all know the extent of the increasing role of computers in our day-to-day life. Hence there is a much greater need to know how to make IT much more secure.

The magazine will try to cater to a wide reading public interested in an enlarged spectrum of IT security. I am proud of our CCNews team on their achievement and look forward to their continued effort in the direction of promoting awareness about IT Security to the people at large .

Vinod Jha
Secretary General - CRPCC

CCC News

Issue 0002
30th June 2009

Rakesh Goyal
Editor
editor@cccnews.in

Moiz Mamoowala
Marketing & Sales
moiz@cccnews.in
+919769887077
+919967247000

Published by
CCC Media,
Mumbai, India

News

Content

News

Survey

Education

Content

UK confesses cyber attack capabilities

The UK has the ability to launch cyber attacks but does not use it for industrial espionage like some other countries, minister Lord West has said.

He refused to be drawn on whether it was used for military purposes.

He was speaking as the government launched a new cyber security strategy aimed at combating online attacks.

He told BBC Radio 4's PM programme the UK faced coordinated cyber attacks "on a regular basis" from other countries including Russia and China.

And he confirmed that the British government had approached the Russian and Chinese governments to ask them to stop the attacks.

"We have had a dialogue with them in the past and I wouldn't want to go into what goes on in terms of debate at the moment," he told the BBC.

'Talented people'

Pressed on whether Britain used cyber attacks itself, he said: "We do not go and attack other nations to try and find from them their industrial secrets."

But he added: "I think it would be very silly of any nation not to have an ability to use cyber space for the safety and security of its nation."

Pressed further on Britain's cyber warfare capabilities, he said: "We have an ability to do things and we have got very good and very talented people who have worked on this."

Asked how the UK could criticise other countries for using electronic espionage, when it used such tactics itself, he said: "I think that coordinated attacks on a regular basis to try and get industrial information from a nation is wrong."

He also hit back at Tory claims the government has been slow off the mark in setting up a cyber strategy, saying it had been working on the issue for some time but needed a more coordinated approach as the attacks had become "cleverer".

He claimed the UK was ahead of the rest of the world in its cyber security strategy.

Launching the strategy earlier Lord West, who has been appointed as the UK's first cyber security minister, said the government had recruited a team of former hackers for its new Cyber Security Operations Centre, based at the government's secret listening post GCHQ, in Cheltenham, to help it fight back.

‘Future targets’

They had not employed any "ultra, ultra criminals" but needed the expertise of former "naughty boys", he added.

"You need youngsters who are deep into this stuff... If they have been slightly naughty boys, very often they really enjoy stopping other naughty boys," he said.

He also confirmed that the government had developed the capability to strike back at cyber attacks, although he declined to say whether it had ever been used.

"It would be silly to say that we don't have any capability to do offensive work from Cheltenham, and I don't think I should say any more than that."

The biggest threat was from "state actors," said Lord West, but the threat from terrorists was also growing and he warned that future targets could include key businesses, the national power grid, financial markets and Whitehall departments.

He denied that hackers had successfully broken into government systems and stolen secret information.

'Missed opportunity'

Lord West joined Prime Minister Gordon Brown and Home Secretary Alan Johnson for a visit to Detica, a London consultancy dedicated to tackling the cyber threat.

Mr Brown said: "I think everybody knows the internet has expanded massively, information is flowing around the world, citizens are in danger of being victims of organised crime, there are potentially terrorist attacks on our community, so we are stepping up this strategic unit to look at cyber security."

But Dame Pauline Neville-Jones, for the Conservatives, said the strategy was a "missed opportunity".

"It is impossible to know how significant these announcements are because we do not know what funding will be made available to enhance our ability to tackle cyber threats. It is also not clear how these new cyber security structures fit into the existing national security machinery."

Her colleague in the Commons, Crispin Blunt, called it a "pale imitation" of an initiative launched by US President Barack Obama.

‘Ethics panel’

Lib Dem home affairs spokesman Tom Brake said: "This new cyber security strategy could lead to an extension of the government's invasive counter-terrorism powers which already pose significant threats to our civil liberties.

"The cyber security strategy uses broad, undefined terms that risk creating panic among the public and a demand for further government powers. We must not retreat into a Cold War mentality."

He demanded reassurances from Home Office minister John Hanson that the new unit, which will start work in September and be paid for out of existing budgets, will not be used to spy on ordinary people's internet use.

Mr Hanson said a special ethics panel would be set up to monitor the new unit and the government would work with civil liberties groups, although he declined to say which ones.

"This is about defending civil liberties and ensuring that we protect the liberties of people to enjoy their lives free of crime and free of the terrorist threat," he told MPs.

Mr Brake and Mr Blunt also asked why news of the new unit appeared to have been leaked to the media - prompting Mr Hanson to admit that it had been issued two days early in error and some newspapers had broken an embargo.

Tom Watson, until earlier this month a Cabinet Office minister in charge of digital engagement, said the opposition were missing the point: "There is state-sponsored hacking of key UK information networks on an industrial scale and we have to transform GCHQ into a spy school for geeks who are more cunning than their Chinese counterparts.”

BBC NEWS: 25 June 2009
news.bbc.co.uk

U.S. pressing China "Green Dam" concern on all fronts

WASHINGTON - The United States still hopes it can persuade China to abandon, or at least delay, its plan to require controversial filtering software on new computers, despite growing trade friction over the issue, a U.S. trade official said on Thursday.

"The U.S. government will remain focused on the problem and use diplomatic and other available means as necessary to resolve it," said Debbie Mesloh, a spokeswoman for the U.S. Trade Representative's office one day after top American officials urged Beijing to drop the plan.

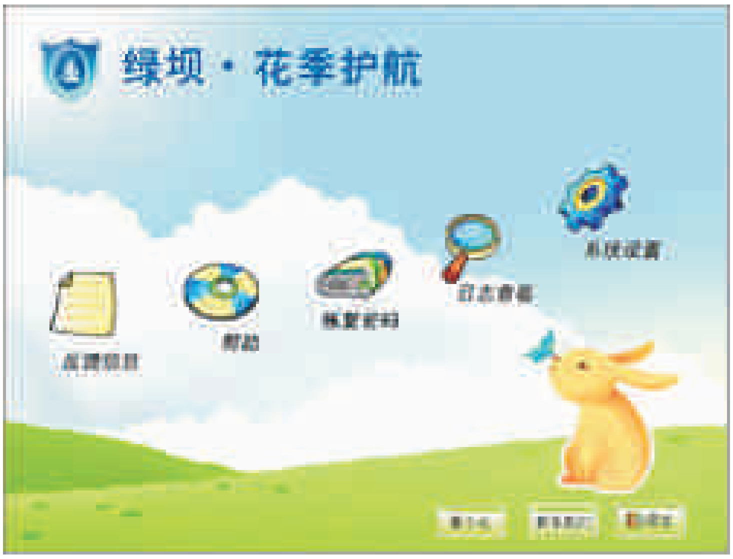
China's Ministry of Industry and Information Technology said on May 19 that all personal computers sold in China must have the "Green Dam" Internet filtering software as of July 1.

Chinese officials said the filter is necessary to prevent children from having access to pornographic websites.

But critics say the software, sold by Jinhui Computer System Engineering Co, is technically flawed and could be used to spy on Internet users and to block sites that Beijing considers politically undesirable.

U.S. Trade Representative Ron Kirk and Commerce Secretary Gary Locke urged China in a letter on Wednesday to abandon the plan, which they said would mean U.S. companies would be required to preinstall software "that appears to have broad-based censorship implications and network security issues."

They objected to the short six-week notice that China gave for the new requirement and said there were complaints from global technology companies and media groups about the software.



If unresolved, the issue is likely to be a sore spot in upcoming U.S.-China meetings, including the Strategic and Economic Dialogue planned for late July, the Joint Commission on Commerce and Trade this autumn and meetings between President Barack Obama and Chinese President Hu Jintao around the Asia-Pacific Economic Cooperation summit in November.

Locke and Kirk also hinted at a possible case at the World Trade Organization, but those can take years to resolve.

One U.S. industry official, who asked not to be identified, said the Obama administration seemed to be emphasizing commercial concerns over the human rights aspect of the issue because China was more likely to respond to that.

The United States exported computers worth about $541 million and computer parts and accessories worth $1.5 billion to China last year. That paled in comparison to the $25 billion in computers and $27 billion in parts and accessories it imported from China in 2008.

Source:Jun 25, 2009, By Doug Palmer

www.reuters.com

US creating cyber-defense command

WASHINGTON - U.S. Defense Secretary Robert Gates on Tuesday ordered the Pentagon to set up a military cyber-command to defend its computer networks against the mounting number of attacks and to develop its own cyber-weapons.

In a memo, Gates told military leaders that the command should be led by the National Security Agency under its current director, Lt. Gen. Keith Alexander, as part of U.S. Strategic Command, which directs computer and nuclear warfare operations.

The decision follows growing concerns over the vulnerability of computer technology as it takes on an increasing role in military operations.

U.S. war doctrine now prioritizes dominance in cyberspace, which Alexander described as the new national security frontier, similar to sea and air power.

The technology available to the United States remains super secret, but the U.S. Department of Defense relies for its operations on 7 million computers and info-tech devices on 15,000 electronic networks.

They come under constant attack. According to the Pentagon, more than 100 foreign intelligence services have tried to hack into U.S. networks.

"Our defense networks are constantly probed. There are millions of scans every day. And the frequency and sophistication of attacks are increasing exponentially," said Deputy Defense Secretary William Lynn.

"The power to disrupt and destroy, once the sole province of nations, now also rests with

A large number of attempted intrusions have been traced back to China, which U.S. officials say has developed a cyber-warfare program. A large number of attacks have also originated from Russian sources.

Hackers have reportedly breached the computer networks of contractors building the F-35 stealth fighter plane. And U.S. troops and civilian staff were banned from using external memory drives after thousands of Defense Department computers were infected by malicious software.

The command will likely be located at Fort Meade, Md., and is scheduled to begin in October and be fully up and running by October 2010.

Trying to downplay concerns that the new command may snoop on civilians, the Pentagon stressed that the developments would only have military applications and that it would not be taking over security efforts for civilian networks from other government agencies.

"This is an internal reorganization," said Air Force Lt. Col. Eric Butterbaugh, a Pentagon spokesman. "It's about the department improving its focus on military networks to better consolidate and streamline (Pentagon) cyber capabilities into a single command."

The Pentagon has thousands of staff directly involved in cybersecurity, and Gates plans to graduate some 200 officers annually.

http://www.upi.com
June 24, 2009

Google slammed as China and U.S. quarrel over Internet

BEIJING (Reuters) - China on Thursday stepped up accusations that Google is spreading obscene content over the Internet, a day after U.S. officials urged Beijing to abandon plans for controversial filtering software on new computers.

The growing friction over control of online content threatens to become another irritant in ties at a time the world is looking for the United States and China to cooperate in helping to pull the global economy out of its slump.

China's Foreign Ministry on Thursday accused Google's English language search engine of spreading obscene images that violated the nation's laws, less than 24 hours after disruptions to the company's search engines and other services within China.

Spokesman Qin Gang did not directly say whether official action was behind the disruptions, but he made plain the government's anger and said "punishment measures" taken against Google were lawful.

"Google's English language search engine has spread large amounts of vulgar content that is lascivious and pornographic, seriously violating China's relevant laws and regulations," he told a regular news conference.

A spokesman for Google in China declined to comment.

Separately, U.S. Commerce Secretary Gary Locke and U.S. Trade Representative Ron Kirk on Wednesday voiced concerns over the "Green Dam" software in a letter to Chinese officials.

"China is putting companies in an untenable position by requiring them, with virtually no public notice, to pre-install software that appears to have broad-based censorship implications and network security issues," Locke said in a statement.

China says the "Green Dam" filtering software is to protect children from illegal images and insists the deadline of July 1 for new computers to be sold with the software will not change.

An official at the Chinese Ministry of Commerce, which handles trade rows, said the ministry had no immediate response to the U.S. criticism and referred questions to the Ministry of Industry and Information Technology, which also had no comment.

Critics have said the program, sold by Jinhui Computer System Engineering Co, is technically flawed and could be used to spy on users and block sites Beijing considers politically offensive.

The proposed new rules raised fundamental questions regarding the transparency of China's regulatory practices and concerns about compliance with WTO rules, the U.S. officials said.

GOOGLE DISRUPTED

The software plan coincides with criticisms of Google by China's Internet watchdog and access disruptions in China to the U.S. company's websites.

The watchdog last week ordered the world's biggest search engine to block overseas websites with "pornographic and vulgar" content from being accessed through its Chinese-language version.

Late on Wednesday evening, Internet users in China were unable to open several Google sites for around an hour, and some reported disruptions throughout Thursday.

A company spokeswoman at Google in the United States said the firm was checking reports of problems with access in China.

The disruption -- coming soon after Google was criticized by China -- "seems beyond mere coincidence," said Mark Natkin, Managing Director of Marbridge Consulting, a Beijing-based company that advises on telecommunications and IT.

Google's problems reflect the difficulties of foreign Internet firms competing in the world's biggest online market while facing controversy over censorship.

Chinese officials have said their Internet moves are driven by worries about exposing children to disturbing online images, but an official newspaper reported on Thursday that a plan to recruit volunteers to scour the Internet for banned content and report to officials also has a political element.

The Legal Daily reported that 10,000 volunteers sought by Beijing would also search for "harmful content" that includes "threats to state security," "subverting state power," and "spreading rumours and disturbing social order."

Natkin, the consultant, said the official pressure was most unlikely to deter Google and other Internet companies from continuing to operate in China.

“Google has to be looking at China as a long-term play," he said. "The allure of the Chinese market, not just for Google and not just for Internet companies, is so compelling, so alluring.”

Source: Jun 26, 2009, Chris Buckley and Emma Graham-Harrison
http://www.reuters.com

EC wants pan-European agency to run security systems

The European Commission has proposed setting up an agency to manage the region's large IT systems containing passport, visa and fingerprint information.

These are the Schengen Information System (SISii) containing passport data, the visa information system (VIS) and Eurodac fingerprint comparison system.

The agency will cost an estimated €113m, but the EC said managing the three systems in one location will lower costs, increase efficiency and improve information sharing.

Annual connection costs are estimated at €16.5m, which will be paid out of the EU general budget.

The agency will be set up between 2010 and 2013 as an independent regulatory body responsible for keeping the IT systems under its charge running without

The agency will also be tasked with ensuring the security, data quality and data protection compliance of the systems.

The plan is to gradually extend the agency to include other systems to become a centre of excellence for security-related IT systems.

The EC said the agency could also be used to prepare, develop and manage future large-scale IT systems in the region.

Source: Warwick Ashford, 25 Jun 2009
http://www.computerweekly.com

Cyber-Criminals Abusing Iran's Political Crisis, Distributing Malware

While the media reports of how the opposition political party in Iran is adopting social-networking websites, particularly 'Twitter' to circumvent government regulation of news relating to the recent presidential election and the successive protests, an Internet security expert is cautioning surfers of cyber-criminals who are taking advantage of the crisis and distributing malware.

John Bambenek, security researcher at SANS Internet Storm Center has this alert for those who might be clicking web-links presented inside random 'tweets' regarding current events in Iran. SecurityManagement reported this on June 16, 2009.

As mentioned, related malware attacks are occurring to redirect users onto malicious websites. Twitter and other social-networking websites are opening doors for cyber-criminals to distribute malicious software since they are allowing anyone to create a blogging site and equip it with posts regarding the political crisis, along with a couple of borrowed images depicting the clashes.

Further some Tweets are traveling across the Web depicting captions, which talk of presenting live situations of protestors facing gun shots. But these tweets connect to different blogs, which contain pre-tested malicious programs that, understandably, many anti-virus software are unable to detect.

Security researchers elucidate that social-networking software and Twitter provide one more mechanism that draws users towards the cyber-attack that previously involved only e-mails i.e. the absence of anti-spam utilities that let anyone's writing on a topic to get displayed.

Thus, while answering an interview for al-Jazeera, a reformist opponent of President Mahmoud Ahmadinejad stated that for them the Net acted just as an air force that functioned during a military maneuver i.e. blasting the camps of the enemy and creating the opportunity for attacking the infantries, in their case their activists, for victory.

Further the Twitter problem is also in its lack of getting to know a particular message's authenticity, as Twitter would display anybody's opinion on a subject. Besides, Twitter has no tool to evaluate the standing of an individual who posts information. Nevertheless, the number of tweets and followers helps, but since the majority of users making posts, though has hundreds of followers, yet they are too trivial a number even before the first tweet.

27 June 2009
http://www.spamfighter.com

U.S. and Russia Differ on a Treaty for Cyberspace

The United States and Russia are locked in a fundamental dispute over how to counter the growing threat of cyberwar attacks that could wreak havoc on computer systems and the Internet.

Both nations agree that cyberspace is an emerging battleground. The two sides are expected to address the subject when President Obama visits Russia next week and at the General Assembly of the United Nations in November, according to a senior State Department official.

But there the agreement ends.

Russia favors an international treaty along the lines of those negotiated for chemical weapons and has pushed for that approach at a series of meetings this year and in public statements by a high-ranking official.

The United States argues that a treaty is unnecessary. It instead advocates improved cooperation among international law enforcement groups. If these groups cooperate to make cyberspace more secure against criminal intrusions, their work will also make cyberspace more secure against military campaigns, American officials say.

“We really believe it's defense, defense, defense,” said the State Department official, who asked not to be identified because authorization had not been given to speak on the record. “They want to constrain offense. We needed to be able to criminalize these horrible 50,000 attacks we were getting a day.”

Any agreement on cyberspace presents special difficulties because the matter touches on issues like censorship of the Internet, sovereignty and rogue actors who might not be subject to a treaty.

United States officials say the disagreement over approach has hindered international law enforcement cooperation, particularly given that a significant proportion of the attacks against American government targets are coming from China and Russia.

And from the Russian perspective, the absence of a treaty is permitting a kind of arms race with potentially dangerous consequences.

Officials around the world recognize the need to deal with the growing threat of cyberwar. Many countries, including the United States, are developing weapons for it, like “logic bombs” that can be hidden in computers to halt them at crucial times or damage circuitry; “botnets” that can disable or spy on Web sites and networks; or microwave radiation devices that can burn out computer circuits miles away.

The Pentagon is planning to create a military command to prepare for both defense and offensive computer warfare. And last month, President Obama released his cybersecurity strategy and said he would appoint a “cybersecurity coordinator” to lead efforts to protect government computers, the air traffic control system and other essential systems. The administration also emphasizes the benefits of building international cooperation.

The Russian and American approaches — a treaty and a law enforcement agreement — are not necessarily incompatible. But they represent different philosophical approaches.

In a speech on March 18, Vladislav P. Sherstyuk, a deputy secretary of the Russian Security Council, a powerful body advising the president on national security, laid out what he described as Russia's bedrock positions on disarmament in cyberspace. Russia's proposed treaty would ban a country from secretly embedding malicious codes or circuitry that could be later activated from afar in the event of war.

Other Russian proposals include the application of humanitarian laws banning attacks on noncombatants and a ban on deception in operations in cyberspace — an attempt to deal with the challenge of anonymous attacks. The Russians have also called for broader international government oversight of the Internet.

But American officials are particularly resistant to agreements that would allow governments to censor the Internet, saying they would provide cover for totalitarian regimes. These officials also worry that a treaty would be ineffective because it can be almost impossible to determine if an Internet attack originated from a government, a hacker loyal to that government, or a rogue acting independently.

The unique challenge of cyberspace is that governments can carry out deceptive attacks to which they cannot be linked, said Herbert Lin, director of a study by the National Research Council, a private, nonprofit organization, on the development of cyberweapons.

This challenge became apparent in 2001, after a Navy P-3 surveillance plane collided with a Chinese fighter plane, said Linton Wells II, a former high-ranking Pentagon official who now teaches at the National Defense University. The collision was followed by a huge increase in attacks on United States government computer targets from sources that could not be identified, he said.

Similarly, after computer attacks in Estonia in April 2007 and in the nation of Georgia last August, the Russian government denied involvement and independent observers said the attacks could have been carried out by nationalist sympathizers or by criminal gangs.

The United States is trying to improve cybersecurity by building relationships among international law enforcement agencies. State Department officials hold out as a model the Council of Europe Convention on Cybercrime, which took effect in 2004 and has been signed by 22 nations, including the United States but not Russia or China.

But Russia objects that the European convention on cybercrime allows the police to open an investigation of suspected online crime originating in another country without first informing local authorities, infringing on traditional ideas of sovereignty. Vladimir V. Sokolov, deputy director of the Institute for Information Security Issues, a policy organization, noted that Russian authorities routinely cooperated with foreign police organizations when they were approached.

This is not the first time the issue of arms control for cyberspace has been raised.

In 1996, at the dawn of commercial cyberspace, American and Russian military delegations met secretly in Moscow to discuss the subject. The American delegation was led by an academic military strategist, and the Russian delegation by a four-star admiral. No agreement emerged from the meeting, which has not previously been reported.

Later, the Russian government repeatedly introduced resolutions calling for cyberspace disarmament treaties before the United Nations. The United States consistently opposed the idea.

In late April, Russian military representatives indicated an interest in renewed negotiations at a Russian-sponsored meeting on computer security in Garmisch, Germany.

John Arquilla, an expert in military strategy at the Naval Postgraduate School in Monterey, Calif., who led the American delegation at the 1996 talks, said he had received almost no interest from within the American military after those initial meetings. “It was a great opportunity lost,” he said.

Unlike American officials who favor tightening law enforcement relationships, Mr. Arquilla continues to believe in cyberspace weapons negotiations, he said. He noted that the treaties on chemical weapons had persuaded many nations not to make or stockpile such weapons.

The United States and China have not held high-level talks on cyberwar issues, specialists say. But there is some evidence that the Chinese are being courted by Russia for support of an arms control treaty for cyberspace.

“China has consistently attached extreme importance to matters of information security, and has always actively supported and participated in efforts by the international community dedicated to maintaining Internet safety and cracking down on criminal cyber-activity,” Qin Gang, spokesman for the Foreign Ministry, said in a statement.

Whether the American or Russian approach prevails, arms control experts said, major governments are reaching a point of no return in heading off a cyberwar arms race.

By JOHN MARKOFF and ANDREW E. KRAMER
http://www.nytimes.com

Despite economic gloom, security Market grows

Security-software market shrugs off economy

While a variety of industries are suffering under the deepest downturn since World War II, the security-software industry appears to be weathering the current economic storm, according to business-intelligence firm Gartner.

The worldwide security market tallied up $13.5 billion in revenue in 2008, jumping nearly 19 percent compared to the previous year, the firm said on Monday. Increasing demand for application-based products, particularly in the e-mail-security and secure-Web-gateway segments, drove the growth, Gartner said. The economy, however, has made sales tougher to close.

"During times of economic uncertainty and budget restrictions, IT security leaders increasingly need to show business value and cost-effectiveness for security measures, and this has impacted and slowed sales cycles," said Ruggero Contu, principal research analyst at Gartner. "However, new product delivery methods, such as software as a service (SaaS) and host based offerings, and expected increasing interest from the small and midsize business (SMB) sector will sustain growth in the market in 2009."

The top-five security-software companies all increased their revenue in 2008, but only McAfee increased its share of the market, and that only by 0.1 percent. Symantec, the owner of SecurityFocus, topped the list, but its market share fell to 22.0 percent from 24.4 percent in 2007, Gartner's data indicated. Eastern Europe was the fastest growing region, logging 35 percent growth, but North America and Western Europe still accounted for more than 76 percent of the market.
Gartner forecasted that the security-software market will continue to grow in 2009, but at a slower rate of about 9 percent.

Source: Robert Lemos, 2009 June 22

TJX to pay $9.75 million for data breach investigations

TJX Companies, Inc., which has undergone a barrage of lawsuits as a result of a massive data breach of its systems, agreed to pay $9.75 million, settling a lawsuit brought on by Attorneys Generals from 41 states.

The parent company of T.J. Maxx and Marshall stores, disclosed in January 2007 that its systems were hacked, exposing at least 45.7 million credit and debit cards to possible fraud. Under the terms of the settlement, the company will pay $2.5 million to create a data security fund for states and a settlement amount of $5.5 million and $1.75 million to cover expenses related to the states' investigations.

In addition, TJX said it agreed to certify that TJX's computer system meets detailed data security requirements specified by the states; and encourage the development of new technologies to address systemic vulnerabilities in the U.S. payment card system.

"Under this settlement, TJX and the Attorneys General have agreed to take leadership roles in exploring new technologies and approaches to solving the systemic problems in the U.S. payment card industry that continue to plague businesses and institutions and that make consumers in the United States worldwide targets for increasing cyber crime," Jeffrey Naylor, chief financial and administrative officer of TJX said in a statement.

Naylor reiterated TJX stance throughout the incident that the company did not violate any consumer protection or data security laws. "The decision to enter into this settlement reflects TJX's desire to concentrate on its core business without distraction and to promote cyber security measures that will benefit all consumers," the company said.

According to investigators, over an 18-month period, hackers exploited a hole in TJX's Wi-Fi network and used a modified sniffer program to monitor and capture data from TJX's transaction systems. Investigators said TJX was using the Wired Equivalent Privacy (WEP) encryption protocol, an older security standard. Wi-Fi Protected Access (WPA) replaces the original WEP security standard. It is compatible with the latest standard, IEEE 802.11i, referred to as WPA2.

Eleven indictments were announced by the United States Attorney in 2008. To date, two of those indicted have pled guilty and two other individuals have pled guilty to related charges.

"This was a self inflicted wound and certainly TJX has done a lot of work since the breach, but the breach itself was the result of poor processes and negligence," said Jon Oltsik, senior analyst, Enterprise Strategy Group.

Although TJX had become the poster child of what could happen when a company suffers a massive breach, Oltsik said it will likely take a breach of intellectual property and other sensitive data that puts a company out of business, before every firm takes data security seriously. There have been other massive breaches since, Heartland Payment Systems is in the midst of a data breach investigation affecting millions of cardholders and Hannaford Supermarket investigators discovered malware that bilked 4.2 million credit and debit card numbers from the grocer's systems.

"The difference between TJX and any other company is just the luck of the draw. They had areas where they were not compliant with PCI but most companies do if you look close enough," said Ed Moyle, cofounder of IT consultancy Security Curve, security solutions manager at integrator CTG. "Some of these environments are quite complex, especially with brick and mortar retail outlets."

The Payment Card Industry Data Security Standards (PCI DSS) have addressed security of cardholder data. But Oltsik said its unclear how much fraud there is in the audit process as there is relatively little oversight from people outside the payment transaction industry.

"PCI is a pretty good first start, but there's plenty of room for abuses and for fraud," Oltsik said.

Lawmakers have gotten involved with dozens of states passing data breach notification rules and two states, Massachusetts and Nevada targeting data security with encryption rules. The federal government has approached the problem on an industry basis, clamping down on the healthcare industry with stronger HIPAA rules and addressing problems in the financial industry. By contrast, the European Union has approached the issue taking a privacy approach.

In December 2007, TJX settled a lawsuit from dozens of banks, agreeing to pay out $40.9 million to cover costs connected to the retailer's massive data breach The banking groups claimed in a lawsuit that the breach compromised 94 million accounts, far more than the 45.7 million figure announced by TJX.

The company also settled various class-action lawsuits brought on by customers who claimed they were victims of the breach. The company agreed to offer affected customers three years of credit monitoring services and identity theft insurance.

Source: By Robert Westervelt, News Editor, 24 Jun 2009
SearchSecurity.com

Google Goes After Malware In Ads

Google has introduced a new search site called Anti-Malvertising.com in an effort to help its ad network partners flag potential providers of malicious advertisements.

The company launched an initial custom search engine at the beginning of the year, aimed at allowing ad networks to do background checks on potential advertisers to reduce the risk of malware.

"It checks a variety of independent, third party sites that track possible attempts to distribute malware through advertising," it says on the site.

"Its search results should not be considered the last word on a prospective customer, but one potential source of helpful information. If a party you're researching comes up in a search result here, we recommend you take a closer look at the party in question before rendering judgment."

The Anti-Malvertising.com site recommends for publishers to always perform in-depth quality assurance on creatives and that they avoid ad networks without strong anti-malware security measures in place.

In early 2008, Google found that about 2 percent of malicious websites were distributing malware via advertising, based on an analysis of nearly 2,000 advertising networks. In a first quarter 2007 Web Trends Security Report released by Finjan found that about 80 percent of malicious code came from online ads.

"The world of online advertising, like the offline world, is a dynamic environment that contains a diverse mix of people with different goals-both good and bad," the site reads.

“This website focuses on malvertising (the threat of malware being distributed through advertising) and how you can help prevent it.”

Source: Mike Sachoff, 2009 June 22
http://www.securitypronews.com

Microsoft Security Essentials Beta Now Available

Once known as "Morro," Microsoft Security Essentials is the anti-malware component of Microsoft's subscription security service, Windows Live OneCare.

Microsoft on Tuesday released a beta version of Microsoft Security Essentials, the company's new free consumer security software.

Formerly known as "Morro," Microsoft Security Essentials is essentially the anti-malware component of Microsoft's subscription security service, Windows Live OneCare, without the utility applications and the $50 annual fee.

In November, Microsoft said that it planned to stop offering Windows Live OneCare to focus on a product that would serve consumers better. Windows Live OneCare will no longer be available as of next week.

Microsoft Security Essentials runs on Windows XP, Windows Vista, and the forthcoming Windows 7 operating system. It's designed to have a smaller footprint and to demand less computing power so it can be used on less-powerful PCs and in low-bandwidth situations. The result for consumers is likely to be a better use experience.

Alex Eckelberry, CEO of Sunbelt Software, a company focused on enterprise security, said he believes that Microsoft knows that it needs to make Windows more secure.

"The fundamental problem that I think Microsoft is trying to deal with is they have a huge PR problem against Apple and Linux," he said. "The fact that you're running Windows opens you up to more attacks because it's a better economic model for malware authors." economic incentive there.

Microsoft Security Essentials "is really for personal use only," said Eckelberry. "On the enterprise side, you shouldn't be affected by this." However, for security vendors with a significant consumer footprint, he believes there's cause for concern. Consumer-oriented security companies, he says, will have to work harder to develop functionality not available from Microsoft.

There are signs that such companies are concerned already. In a blog post on Tuesday, David Harley, director of malware research for ESET, dismisses Microsoft Security Essentials as insufficient. "This isn't full-strength anti-malware (and is unlikely to be when it leaves the beta testing stage) any more than the Windows firewall is a full-strength firewall system, which means that it isn't going to render the anti-malware industry redundant," he said.

But what Microsoft's software may do is reduce the number of unprotected Windows PCs, leaving less low-hanging fruit for unskilled attackers.

Source: Thomas Claburn, InformationWeek, June 23, 2009

http://www.informationweek.com

Cyber-criminals can help to catch cyber-criminals

Police want to tap up past offenders to battle-against-cyber-crime

A senior police officer has suggested that the best way to compete against cybercrime is to work with those jailed for high-tech offences.

Detective Superintendent John Mooney, of the National Police Improvement Agency (NPIA), believes that online crime can only be countered effectively if past offenders help broaden the police's knowledge base.

Getting into fraud techniques

"We are behind, especially where technology is involved, and this will help us to chase that group. If a tactic was to get some of these people to sit down and explain their methods to us post conviction, I am quite sure that would help," said Mooney

"To look forward 10 years we also have to look back and ask some of these people, for example, how did you transform this credit card into a workable card?

“Everybody will benefit if we manage to get into some of this fraud technology because it will mean people pay less insurance.”

Source 24 June 2009.
http://www.techradar.com

Hackers seizing control of RSS feeds

If you use RSS feeds, be advised that there may be hackers out there that are taking control and redirecting users to spammer sites.

According to an article on seroundtable.com there has been a rise in the number of RSS feeds being hacked into lately.

Wordpress feeds were cited as one place where these feeds are being compromised.

If you have sites that use RSS feeds, you may want to check them now, and monitor them regularly.

June 25, 2009.
http://www.examiner.com

News homepage
Events homepage
RSS
Automated feed from Northland Regional Council
Your RSS Reader
Your RSS news reader provides you links directly back to the news on our website

Can you trust your vendor?

Router backdoors put businesses at risk

Businesses and government systems are at risk from undocumented administrator accounts that provide a backdoor for unauthorised access.

An Ovum report entitled Can you trust your vendor? has revealed undocumented privileged administrator accounts in new network routers belonging to two telecoms service providers.

"This is not the first time that we have seen attempts to hack into enterprise and carrier networks by infiltrating network routers," says Graham Titterington, information security principal analyst at Ovum.

The unauthorised accounts were found by accident as most security audits do not check privileged admin accounts, says Titterington. He recommends that companies concerned about backdoors in their network routers check that there are no unauthorised privileged accounts.

Backdoors in routers used to be quite common, says Richard Brain, technical director at security firm Procheckup. "In 1999, certain Cisco routers had a backdoor maintenance account to reset passwords. Lots of backdoors have now been removed."

However, in 2006 Cisco "forgot" about the backdoor account on its Cisco Security Monitoring, Analysis and Response System. The company issued a workaround.

Although many router backdoors have been plugged, there is a bigger problem with backdoors in software, such as the system software providers use for online error reporting and remote maintenance.

Chris Wysopal, CTO of Veracode, a company which specialises in analysing software for security holes, warns that such backdoors are very common. "We find that hard-coded admin accounts and passwords are the most common security issue."

The problem here is that the servers software suppliers use for collecting the errors and for distributing software updates over the internet, may be attacked. This could lead to compromised code being installed via the legitimate maintenance "backdoor" suppliers use for auto updates. In 2001 the Apache Foundation servers which host open source code were targeted by such an attack.

"CIOs need to check with software suppliers that any special admin accounts built into the product are disabled," Wysopal says. Open source code is prone to abuse, where backdoor code can easily be inserted into the source code. However, Wysopal says the rogue code is often identified quickly, within a few days, and is removed.

Commercial, closed source software, is more problematic. Programmers with links to organised crime may slip through the vetting net and find ways to hide backdoors in commercial products, which Wysopal says can be extremely difficult to find.

The only sure way to prevent backdoor hacking attacks is to eradicate backdoors. Admin accounts should only be assigned to internal staff, based on their job role, and suppliers must be forced to reveal the backdoors built into their products.

Source: Cliff Saran, 25 Jun 2009
http://www.computerweekly.com

Over 2.7 Billion Vulnerable Programs Installed on US Computers

According to statistics gathered by Secunia's Personal Software Inspector

Secunia claims US Internet users have over 2.7 billion vulnerable programs installed on their computers

Reputed Danish vulnerability intelligence provider Secunia has recently released version 1.5 of its free Personal Software Inspector (PSI) application. Statistics gathered by the software reveal frightening numbers, such as 2,720,800,000 vulnerable programs being installed on U.S. computers.

Secunia PSI is a free application that scans the programs installed on a computer in order to determine if they are affected by any security vulnerabilities. In order to make this assessment, PSI queries the company's database of security advisories, one of the most complete in the world.

If an application is found to be vulnerable, PSI verifies if any update or newer version that might fix the issue is available and provides the user with a direct download link to it. The tool also tags programs that reached their end of life and are no longer supported by their developers, as a security risk.

According to Secunia, there is an estimated number of 227 million Internet users in the United States, out of which about 400,000 have scanned their computers with PSI. The company notes that PSI users currently have an average of four unpatched programs installed, while the average US Internet users have 12 such applications on their computers.

"The fact that US based PC users have more than 2.7 billion vulnerable programs installed are shocking! And quite frankly I am very surprised, we had an idea it would be bad, but couldn't imagine the enormous scope of this problem. And to make things even worse, the picture formed in the US is the same all over the world," Mikkel Winther, manager of Secunia's PSI Partner Program, noted.

Secunia's statistics seem to be consistent with the malware distribution trends observed in recent times. Cyber-criminals have come to rely more and more on vulnerabilities in order to infect computers. And not just the ones affecting the Windows operating system itself, but other popular programs as well, such as Adobe Flash Player, Adobe Reader, Mozilla Firefox, Opera, Internet Explorer, PowerPoint, Word, and so on.

"PC users need to patch! They need to patch all their vulnerable programs and they need to do so as fast as possible after the patch has been issued from the vendor. Failing to do so is playing Russian Roulette with your IT security – it is only a question about time – and luck – when your system will be compromised," Mr. Winther advised.

Source: By Lucian Constantin, 25th of June 2009.

Cyber hackers target Michael Jackson fans

Cyber criminals and online hawkers kicked into action within minutes of hearing the news of Michael Jackson's death.

Just as they harnessed the hysteria over swine flu and the impending end to the tax year, online miscreants seized on the pop star's death to hook people into opening malware-laced spam emails, web security companies reported.

One set of spam emails, discovered by Websense, purports to offer unpublished videos and pictures of Jackson, but the link in the email is not of a YouTube clip but instead leads to password-stealing malware that installs on the victim's computer.

Unusually, Websense reported there was an Australian link: "This [malicious] file is located on a legitimate website hosted in Australia belonging to a radio broadcasting station." Further details about the radio station are being sought from Websense.

Trend Micro observed that scammers were also using "black hat" search engine optimisation techniques to push their malicious websites close to the top of search results.

McAfee said spam offering news or pictures relating to deceased celebrities - Jackson and Farrah Fawcett being this week's most popular targets - often led to malicious websites or sites offering knock-offs of drugs such as Viagra.

The King of Pop's death sparked an unprecedented rush to the web as the world digested the news, with Google reporting it initially interpreted the spike in traffic to its Google News service as an attack by hackers.

Source: Asher Moses, June 29, 2009
http://www.smh.com.au

Roaming fraud will cost $5b annually

MACH, which provides solutions for the mobile supply chain, warned that it expects roaming fraud to cost mobile operators $5 billion globally in 2009 as many operators around the world have yet to comply with Near Real Time Roaming Data Exchange (NRTDE) recommendations developed by GSMA. Consequently, fraud will shift to those who are less well protected, as it always does.

“Perpetrators of roaming fraud rely on poor operator visibility and slow inter-operator processes to profit at the operators' expense,” says James Stewart, Director of Fraud Product Management at MACH and Chairman of the Roaming Sub-Group of the GSMA Fraud Forum.

He adds, “Many operators are re-evaluating the use of their existing fraud detection measures, looking for ways to reduce expenditure. Their margins are under pressure from increasing roaming tariff regulation and competition but they cannot afford to increase their exposure to fraud and their subscribers will not accept any disruption to service caused by fraud prevention."

MACH clears two out of every three roaming calls on GSM and CDMA networks and settles more than 60% of global inter-operator wholesale invoice amounts. MACH has over 300 NRTRDE clients, and a rapidly growing Fraud Protection client base that is doubling every six months.

May 26, 2009
http://www.telecomseurope.net/

Control 1000 PCs for Five Dollars

Zombie attacks on sale for a fiver
Golden Cash a "milestone in the cybercrime evolution"

Researchers at security firm Finjan said on Wednesday that they have uncovered an underground botnet-leasing network where cyber criminals can pay $5 to $100 to install malware on 1,000 PCs for things like stealing data and sending spam.

The Golden Cash network, dubbed "Your money-making machine" on its homepage, sells access to botnets comprised of thousands of compromised PCs to cyber criminals for custom malware spreading jobs, according to issue two of the Cybercrime Intelligence Report for 2009.

Here's how it works: a cyber criminal creates a botnet by hiding malicious code in a legitimate website that is used to turn web surfing PCs into zombies. The code, typically an iFrame, points the PCs to a separate website where they are then infected with a Trojan backdoor that reports back to the Golden Cash command and control server.

In order to increase the number of botnets, the Golden Cash server installs an FTP (file transfer protocol) grabber on new zombies to steal credentials used by the computers to run websites, giving the server control over additional legitimate websites. Approximately 100,000 domains, including corporate domains from around the world, were identified among the stolen FTP credentials under Golden Cash's control, according to the report.

Customers pay for the ability to install different types of malware on the Golden Cash bots, which are recycled for new jobs and new customers afterwards. Prices are higher for compromised PCs in western countries, the report said.

"This advanced trading platform marks a new milestone in the cybercrime evolution," Finjan said in a statement.

More technical analysis is available on Finjan's Malicious Code Research Center blog, including the fact that the command and control server is hosted in Texas, the registrant country is China and the "proxy" website that tunnels traffic to the command and control server is hosted in Krasnodar, Russia.

Source: By Elinor Mills, 18 June 2009
http://software.silicon.com

Tackling cyber crime together

Cyber crime costs the EU billions of euros each year – but to defeat it, we need better co-operation between member states

Gordon Brown has announced the creation of a new UK cyber-security centre to combat growing attacks on computer systems within government departments and big business. Police forces are planning to set up regional "cyber crime" squads on anti-terrorist lines. Brown's initiative follows an earlier move by Barack Obama to appoint a US "cyber tsar".

Britain has been holding talks with the US and Canada to co-ordinate operations against cyber-attacks by foreign powers, terrorists and criminals. But there is growing evidence of the need for a truly pan-European response to what is a rapidly accelerating threat across the whole of the EU – and to its businesses and 500 million citizens.

Organised criminal groups are using the internet to attack a large number of European citizens and businesses for huge gains. But the widely different jurisdictions and legal systems in the EU make it almost impossible for law enforcement agencies and the judiciary to successfully investigate and prosecute a pan-European criminal case. That's what has come home to me after taking part in the prosecution of more than 400 criminal cases.

The focus at the EU policymaking level is on protecting what is called critical information infrastructure, such as electricity grids. But what policymakers also need to do is find mechanisms to address organised cyber crime in Europe. It's so easy to move from one country to another and there are certainly no borders on the internet – but there are borders when it comes to judicial co-operation. That's the biggest challenge that Europe needs to address.

The EU is committed to rolling out high-speed broadband connections to all its citizens – a top priority for Viviane Reding, the EU information society and media commissioner. Unfortunately, while the internet offers great opportunities in our daily lives and in business, it is increasingly used for illegal gains. So we need to find common solutions that make it hard for online criminals to defraud businesses and consumers, download illegal content, move funds illegally etc.

Reding is also pressing the EU to appoint its own cyber tsar, primarily to combat attacks on infrastructure such as those in Estonia, Lithuania and Georgia in the past two years. This was the main topic of a cyber warfare conference this month in Tallinn, the Estonian capital, where EU ministers initially discussed it in late April.

But it's clear that gaps in judicial co-operation in Europe are creating a paradise for internet fraud. It's also clear that the majority of cyber threats in Europe are not related to cyber warfare but to cyber fraud, a much bigger and more widespread phenomenon – and growing exponentially. A typical example of a fraudulent scheme would be: fraudster X masterminds a criminal ring in, say, Italy organising cross-border phishing (sending spoof emails) attacks from several EU countries that target financial institutions and e-commerce globally. By recruiting online "money mules" in other countries to move the money from one jurisdiction to another and paying them a small fee X creams the bulk of the huge profits. Fraudsters are even creating their own ISPs (internet service providers) to use the IPs (internet protocols) for their criminal activities.

The protection of EU citizens and businesses resides or should reside with the European commission's justice, freedom and security directorate-general. Radomir Jansky, an official responsible for cyber crime there, told a recent Amsterdam conference of the messaging anti-abuse working group that there was an urgent need to strengthen cross-border co-operation between law enforcement agencies and private industry – and increase penalties for cyber crime from the current one to three years in EU legislation.

But there's an extraordinary lack of data on the scale of cyber crime in the EU and no unified system for reporting it. Europol is setting up a European platform for reporting crime, but officials admit that the 27 EU member states are under no obligation to provide them with information and they have no precise data on either the scale or the cost of cyber crime in Europe.

What we know is that available statistics show that cyber crime costs $1tn worldwide each year. An April 2009 study by the internet security firm McAfee shows that data theft and other online offences have robbed global businesses of that staggering amount. But Europe's share is unknown.

Online credit card fraud alone cost the UK £223.8m in 2007, according to the online identity protection company Garlik. This type of phishing is rising, with information about cards representing 32% of data illegally available online in 2008 – up from 21% in 2007, according to the internet security firm Symantec. And this is just the tip of the iceberg. We need cross-border co-operation in Europe to fight a borderless crime that puts at risk the benefits of a digital society and economy.

Source: Albena Spasova, 25 June 2009
guardian.co.uk

PC in a plug hits the UK

A computer the size of a plug has been launched this week in the UK.

A computer built into a three-socket plug has been released in the UK by American firm Marvell Technology Group this week.

The "SheevaPlug" allows a customer to plug the device into the wall and use it as a home server. The company claimed it consumes just one tenth of the power compared to using a PC for the same job.

Rob Enderle, principal analyst for the Enderle Group, said in a statement: "The Plug Computer is one of the more amazing technologies that have come out this decade and it has the potential to change the world."

The plug itself contains a Marvell Kirkwood 1.2GHz processor with 512 Mb of NAND flash, 512 Mb of DRAM and a USB 2.0 port. It connects to the home network through Ethernet.

Versions of the plug computer, being targeted at developers, have already been launched in the US but this is its first foray into the European market.

Dr Simon Milner, vice president of the Enterprise Business Unit for Marvell, said: "The wide range of applications created from the open-developer SheevaPlug platform serves both retail product partners and service providers."

"We are thrilled to introduce SheevaPlug to the European developer community and look forward to seeing many new applications and new consumer product ideas developed and brought to market."

Source: Jennifer Scott, 25 Jun 2009
http://www.itpro.co.uk

Canada's IT associations team up for cyber security

A group of five Canadian IT associations have joined forces to launch a national security research group in an effort to advance the country's cyber security strategies.

The Canada Advanced Security Initiative will develop a study, survey and workshop program to develop a new strategic vision for the security industry in Canada and its ability to support users at home and abroad.

The initiative's participants include the Canadian Advanced Technology Alliance, the Canadian Information Processing Society, the Information Systems Audit and Control Association, Association de la sécurité de l'information du Québec and the Canadian Society for Industrial Security.

“Recent events created a huge increase in interest by governments and the private sector in the use of advanced security,” John Reid, the president of the CATAAlliance. “For example, the tightening of the US border security policy makes it imperative that we show our security capabilities.”

http://blogs.itworldcanada.com

UK Government increases Use of Secure File Transfer could help prevent embarrassing data leaks

Over the past decade, the UK Government has increasingly used online technology to deliver and improve public services, whilst seeking to limit public spending. This strategy has enabled many departments to provide a wider range of services in many more formats, assisting people to access Government more easily and effectively. However, there have been some unwelcome consequences, as witnessed by the spate of high profile Government data losses and security breaches. The UK Government could mitigate these kinds of risks by integrating secure, file transfer capabilities into its core processes - allowing data to be transferred safely and prevent further data leaks and loss of personal, confidential information.

In all aspects of the public and private sector, the transition of data from a physical to digital format has been rapid and widespread. Once business and Government exchanged folders, paper and CDs, now they send electronic files online. Communication, data, correspondence, images, texts and archives are now "digital assets" created and maintained electronically; making life easier and data transportation faster and more accurate.

Whilst switching to digital communication has improved speed and efficiency, it has highlighted concerns about the security of data transfer. The value, confidentiality and importance of data in a digital format is exactly the same as physical data. The UK media's ongoing reports of data breaches demonstrate that the Government has not fully grasped the need to secure digital assets with the same degree of protection given to safeguarding physical assets. Since the start of this year, the UK's Information Commissioners Office (ICO) has highlighted more than 140 data security breaches in the NHS alone, with four separate NHS Trusts found to have breached the 1988 Data Protection Act. The Ministry of Defence lost a laptop containing 600,000 records of UK residents, whilst the most high profile data breach of all was the Government's loss of CDs containing personal information on 25 million recipients of Child Benefit in December 2007.

For Government looking to improve services and limit public spending, the Internet is a highly attractive option. As a result, Government has encouraged and facilitated the development and implementation of online systems to deliver services in ways which were unimaginable only a decade ago. Many people now opt to pay taxes, file returns, apply for benefits and manage their personal affairs online using their laptops, PCs, mobile phones and BlackBerrys. Government has always had access to confidential, personal information but until relatively recently, this was mostly paper based. The rise of Internet has seen much more data being transferred electronically using a variety of devices, many of which are not secure. As a result, Government data security systems have sometimes left personal, confidential data more vulnerable to interception, loss and theft.

The UK Government is addressing many of these issues with its Code of Connection (CoCo) Compliance. This defines the minimum standards and processes that Local Authorities must comply with, before they can connect to Government's national communications extranet, which gives them secure communication with other local authorities and organisations.

Achieving compliance to the CoCo requires local authorities to provide a compliance statement and supporting comment against a number of security control measures. CoCo compliant local authorities have access to the Government's secure intranet, through which they can communicate securely with central government departments, other local authorities and other partner organisations.

Until 'Government Connect', the UK Government's national secure network infrastructure is fully implemented, many Departments will continue to use email combined with file transfer protocol systems to transfer data.

Whilst this is an effective solution for some organisations, its security features do not provide the degree of data protection and audit trails which Government Departments need to meet compliance and audit legislation. FTP users have also become adept at circumventing its security features, often sharing a single user-name and password amongst multiple users. This represents a considerable threat the data being transferred. Enhanced FTP systems (such as SFTP, FTPS and EFTP) offer genuine improvements over conventional FTP, but they require specialist programs to be installed on users' desktops. This means additional equipment costs, as well as management overheads for IT departments and inconvenience for users.

Data management over FTP can also be problematic: files are uploaded to FTP directories are rarely deleted, as this requires manual intervention. As a result, FTP systems often contain multiple directories holding hundreds of files, but few have any information about when they should be deleted. The directories represent a valuable digital asset, but they are often ignored or left unused for long periods. As such, they are a soft target for unscrupulous users and a represent a potential security threat.

Traditional solutions like FTP now struggle as adequate tools for secure and large file transfers. With data confidentiality such high profile issue, Government needs to consider a dedicated solution which offers embedded security. Data encryption is essential, and systems should be capable of authenticating the recipient and managing each file and account lifecycle automatically. This would mean that no confidential information is left exposed and no unauthorised user access takes place.

Technologies such as Accellion's managed file transfer solution have emerged to meet the need for on-demand and automated, multi-site, secure file transfer. In the US, many national, federal and local Government organisations have implemented Accellion's solution. This has included the US Department of Health & Human Resources, which is the primary Government healthcare provider, as well as the National Institute of Health, the Government agency responsible for medical research. These and other US Department have deployed the managed service to deliver the security, authentication, encryption, file tracking and reporting capabilities they need to meet their obligations on data and information security, such as the Department of Defence Directive 8500.1 and the Health Insurance Portability and Accountability Act (HIPAA).

The Accellion solution eliminates the risk of data breaches by fully encrypting all files, in addition to controlling access to individual documents. It can securely send and receive files and folders up to 50GB lost on a memory stick by NHS Trust late last year. It is easy to use, can be installed in less than an hour and has minimal impact on IT resources.

The UK Government is currently running a number of pilot projects to assess Accellion's solution. In the US, it is already being used by Government organisations such as NASA, the Port of Los Angeles, Florida's Department of Transport and the Securities and Exchanges Commission (SEC).

As services move increasingly online, the Government's focus must be securing personal data to bolster users' confidence and prevent further damaging data leaks. Secure, managed file transfer has already proven itself an efficient and cost effective solution for Government departments in the United States and Canada. As a sophisticated, effective and unobtrusive solution, it could become a core process, enabling the UK Government to communicate effectively and securely; making embarrassing data breaches a thing of the past.

http://www.securitypark.co.uk/

Study shows high vulnerability of social networkers

Facebook, LinkedIn, MySpace and Twitter users are more vulnerable to financial loss, identity theft and malware infection than they realise, a survey has revealed.

Social networking sites encourage users to behave in risky rays, the survey of more than 1,000 users by security firm Webroot found.

Three in 10 people admitted they had been attacked by cybercriminals through social networking sites in the past year.

These attacks include identity theft, malware infection, unauthorised password changes and friend-in-distress scams.

Yet, two-thirds of respondents said they did not restrict any details of their personal profile from being visible to search engines.

Some 80% allow at least part of their profile to be accessed by search engines and more than half are not sure who can see their profile.

Criminals typically use personal information to guess passwords and access accounts, warned Mike Kronenberg, chief technology officer at Webroot's consumer division.

"A third of those polled said they include at least three pieces of personally identifiable information in their profiles," he said.

Once criminals are able to access accounts they hijack them to send legitimate looking messages containing malware to other members of the social network.

More than a third of respondents said they use the same password across multiple sites, which means if one account is compromised, all others are vulnerable.

This risk is higher among users under 30, where 51% said they used the same password for all online accounts.

Social networkers should use privacy setting to restrict access to personal information, restrict personal information in profiles and use different passwords, said Kronenberg.

"Malware authors are continually writing new programs to avoid detection, so even if users have anti-malware installed, they should remain vigilant," he said.

Source: Warwick Ashford, 26 Jun 2009

Internet will become unreliable next year

Unless the network infrastructure of the internet is upgraded, users will experience slower and unreliable connections by next year.

Growing demand for multimedia content and a growing number of internet users will put pressure on outdated networks and could cause serious problems for businesses.

Websites such as YouTube and the BBC's iPlayer, which use a lot of bandwidth, will make the internet unreliable, new research claims.

According to a report in the Sunday Times, US think-tank Nemertes said as demand for bandwidth potentially doubles, computers will regularly start freezing and dropping offline as early as next year.

Nemertes said the growing number of people working from home will also contribute significantly to the increased demand for bandwidth.

Ted Ritter, an analyst at Nemertes, told the Sunday Times that the internet, without network upgrades, will no longer be reliable enough for business users. "For business purposes, such as delivering medical records between hospitals in real time, it is useless."

The internet will become merely an "unreliable toy," he added.

He said disruption will start next year. At first, computers will jitter and freeze. This will be followed by what he describes as "brownouts"- the combination of computers freezing temporarily and being reduced to a slow speed.

According to website Internet World Stats, internet users totalled almost 1.6 billion in March this year, compared with about 361 million at the end of 2000. There was a 342% increase between 2000 and 2008, and over 23% of the world population now uses the internet.

The Digital Britain interim report, which was published by communications minister Stephen Carter in January, proposes 22 action points to achieve five main goals, including upgrading and modernising the UK's digital networks.

Ismail Ismail, director at Webcredible, which monitors web performance, said, "The problem is that the infrastructure of the web was developed long before sites like BBC iPlayer and YouTube existed and bandwidth is now being eaten up faster than was imagined."

He said Lord Carter's Digital Britain agenda, which aims to get broadband to everyone in the UK by 2012, will make the problem worse.

“If businesses suffer downtime problems and a slow connection, all the good work done by these companies could be undone by something they have no control over, with their previous investment in user experience severely undermined by the lack of bandwidth.”

Source: Karl Flinders, 27 Apr 2009
www.computerweekly.com

CISOs Say Insiders Are Greatest Threat To Data

In study, 80 percent say they're more concerned about employees and contractors

Eighty percent of chief information security officers (CISOs) believe that employees and contractors present a greater threat to their data than external hackers, according to a study released earlier today.

The study, conducted by NetWitness and MIS Training Institute, was conducted at the 6th Annual CISO Executive Summit in Lisbon, Portugal, this month. Only 18 percent of the respondents said they considered hackers or nation-sponsored attacks to be a greater threat than insiders.

One in 10 CISOs reported they are not planning on spending any new monies on security this year, and are trying to just survive with their existing technology investments, the study says.

Twenty-six percent view governance, risk, and compliance (GRC) verification as the primary business driver for security spending in the next 12 months.

One-third of respondents believe firewalls alone provide adequate protection against data leaks. One-quarter of CISOs reported either not having the correct data leakage protection technology, or not knowing what they should have.

“What is really alarming is the misperception that traditional security approaches alone can protect against information leaks," says Sara Hook, conference director for EMEA at MIS Training Institute. Hook also expressed concern that "some CISOs were not sure what they need for data protection, or were not planning to focus any money in that area this year.”

Source: Jun 23, 2009, By Tim Wilson
http://www.darkreading.com

Cyber Security Practices

Back up important files

Backing up the contents or your computer is critical

Our computers contain vast amounts of data in many forms: from family photos and music collections to several years' worth of financial records and personal contacts.

In fact, a recent NSCA/Symantec study found that more than 68% of Americans store more the 25% of their photos digitally. For most people, the loss of that information could be devastating.

There are many risks to our data, such as hardware or software malfunctions, natural disasters and emergencies—floods, hurricanes, tornadoes, house fires, and theft. But viruses, spyware, and cyber attacks are also externally launched events that can lead to data loss and can either destroy your computer or render it useless.

It's not only big events that cause a data loss. Important files can be lost by accidental deletion as well.

Protect yourself against data loss by making electronic copies of important files, commonly referred to as a backupG. Data backup is a simple, three step process:

1. Make copies of the data on your computer(s)
2. Select the appropriate hardware to store the backup data
3. Safely store the backup device that holds your copied files

Read on for further details on each of the steps.

1) Make copies of your data:

There are several software tools you can use to backup your computer. First, check to see if your computer already has backup software program installed; many programs do.

Most backup software tools will allow you to make copies of either everything on your computer (files and computer programs) or just the files you've changed since the last time you conducted a backup (thus you will always have copies of the most up-to-date versions of your files). For more information, see How to decide what data to back up.

Below are links to backup utilities in popular operating systems:

WindowsXP:
http://www.microsoft.com/windowsxp/using/setup/maintain/backupfiles.mspx

Vista:
http://www.microsoft.com/protect/yourself/data/backup.mspx

MAC OS:
http://support.apple.com/kb/HT1553

Other software programs are available for purchase if your system does not have a backup program or you're seeking other features.

Ideally, you should backup your files at least once a week. In some instances you might want to do an immediate backup, such as after you download 1000 family photos from the trip of a lifetime or invest time in digitally archiving your music collection.

2) Select the hardware to store your data

When you conduct a backup, the files will have to be stored on some kind of memory device—external hard drive, CD's, DVD's or USB flash drives (sometimes called thumb drives because of their size).

The option best for you depends on several factors, but the most important question to answer is: How much data do you have to backup?

If you don't store much in the way of music, photos, videos, or other large files and mostly use your system for surfing the web and the occasional document, try using CDs, DVDs (if your computer has a CD or DVD drive that can "write" to that media), or a USB flash drive.

If your computer serves as the family photo and video album as well as your music library, the best bet is to get an external hard drive that plugs into your computer (preferably via a USB port). This way you can assure more adequate storage space for all your files. Copying information will also be faster with these devices. Like most computer hardware, the prices of these devices have been dropping over the years, and become more affordable all the time. When viewed as the cost of insurance to protect you memories, music, and vital information, they seem inexpensive compared to the value of the loss.

If you don't want to hassle with new hardware, there are online backup services available, usually for a monthly fee. You simply backup your files to a secure server over the InternetG. These services have the added advantage of safely storing your files in a remote location (see below) and the files can be accessed anywhere you have a connection to the Internet and they will also be backed up at the remote location by the service provider. Please check to ensure the backup site you choose is a secured one. See How to recognize spoofed Web sites for more information on verifying secure sites.

3) Safely store the backup device that holds your copied files

Now that you have set up the software and started copying your files on a regular basis, you need to make sure you do the last important step: Keep the files on your backup device somewhere safe. The most secure practice is to keep your backed up data offsite. That way, should the unthinkable happen—house fire, natural disaster, or theft—you can recover your valuable files quickly. If you use an online backup service, you've already accomplished this goal.

Keep your backup device close enough so you can retrieve it quickly and easily when you do your REGULAR backup. Some ideas include:

* A trusted neighbor (you store your device at their house and they store theirs at yours).
* A nearby family member or friend.
* Your workplace, if it can be locked up, doesn't violate workplace policies or the law.

If offsite won't work for you, find a secure place in your home that would likely survive any natural disasters. For example, if flooding is a concern, keep the device somewhere above the worst possible flood threat. You may also want to consider keeping your backup in a bolted and/or fireproof box.

Source: http://www.staysafeonline.org

Tips for Staying Safe Online

- All computer users can follow a few simple guidelines to keep themselves safe in cyberspace. In doing so, they not only protect their personal information but also contribute to the security of cyberspace.

- Back up important files.

- Install anti-virus software, a firewall, and anti-spyware software to your computer, and update as necessary.

- Create strong passwords on your electronic devices and change them often. Never record your password or provide it to someone else.

- Ignore suspicious e-mail and never click on links asking for personal information.

- Only open attachments if you're expecting them and know what they contain.

- Delete any e-mail offering you money by lottery or dead person from Africa or government contract. Nobody gives you free money.

Achieving Information Security with ISO 27001

By Anjay Agarwal

The objective of this presentation is to understand the importance of information security and its gravity of importance to an organization. The steps involved in implementing ISMS and conclude with the benefits that an organization can draw by implementing ISMS.

Introduction

In today's business, information is 'THE LIFELINE' for an organization. It is not that information was less important in yesteryears, but the technology has exposed information beyond the requirement. The concern here is the increasing security threats to the organization's and their information systems from a wide range of sources, including computer assisted fraud, espionage, sabotage, vandalism, fire or flood. Computer viruses, hacking and denial of service attacks have become more common and increasingly sophisticated.

Information means "Knowledge derived from any source". ISO/IEC 17799:2005 states that "Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation." Thus, Information is a wider term than Information Technology (IT).

Information Security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investment and business opportunities. The three basic components of Information Security are:

a) Confidentiality – Ensuring that information is accessible only to those authorized to have access
b) Integrity – Safeguarding the accuracy and completeness of information and processing methods
c) Availability – Ensuring that authorized users have access to information and associated assets when required.

I would like to add one more component to this information security which is related to –

d) Fiduciary – Understanding the various acts, rules, regulations, guidelines, professional and industry practice, etc. and protecting against them as well.

Almost all organization implement information security in a way that suits them best. There was need for a systematic approach for implementing information security and also to bench mark the organization's information security against the best practices. ISO 27001 is an International Standard prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the Information Security Management System (ISMS).

ISO 27001 is a process based approach adopting the "Plan-Do-Check-Act" (PDCA) model. This 'process based' approach encourages its users to emphasize the importance of:

a) Understanding an organisation's information security requirements and the need to establish policy and objectives for information security
b) Implementing and operating controls to manage and organisation's security risks in the context of their overall business risks
c) Monitoring and reviewing the performance and effectiveness of ISMS
d) Continual improvement based on objective measurement

Implementing ISMS ISO 27001:2005

How one can achieve ISO 27001:2005 security certification? The steps involved in achieving ISO 27001certification is as under:

1) **Project Scoping**
Proper scoping of an ISMS project is the FIRST step in the compliance initiative for ISO 27001:2005. The organization as a whole or as part that needs to be compliant is to be identified in terms of their characteristics of business, location, assets and technology. It is important that top management is involved while determining the scope since it requires their commitment. This is because they understand their business need and are aware of their risks and therefore their information security needs that are to be achieved.

2) **Initial Gap Analysis**
ISO 27001 has 11 information security domains, 39 Control Objectives and 133 Controls. Besides this, there are mandatory clauses as mentioned in clauses 5 to 8 of the standard. An initial gap analysis is done to determine the extent of compliance vis-à-vis ISO 27001 standard. This would determine the gaps in information security vis-à-vis the standard

3) **Risk Assessment**
Risk assessment is a mandatory component of ISO27001 and would help to analyze the levels of information security risk inherent in your business processes. The steps involved in Risk Assessment are;

1. Define approach to Risk Assessment including the criteria for accepting the risks and identify acceptable level of risks.
2. Identity the information assets, threats to these assets, vulnerabilities that might be exploited by the threats and the impact that losses of confidentiality, integrity and availability may have on these assets
3. Analyse and evaluate the risks by assessing the business impacts that might result from security failures taking confidentiality, integrity and availability of the assets. The probability of the security failures needs to be assessed and the level of risks needs to be estimated taking into account the controls in place. Thereafter, determine whether the risks are acceptable or require treatment.

4. **Risk Treatment**
The primary step in risk treatment would be to classify those risks identified above under risk assessment. Once, it has been decided the risks requiring treatment, the possible alternatives are;
a) Applying appropriate controls
b) Knowingly and objectively accept risks
c) Avoid risks
d) Transferring the risks to third parties
After the risk treatment plan put in place, once again investigate if the treatment meets the desired objectives. There would be a certain percentage of residual risks for which management approval should be taken.

5. **Vulnerability Assessment and Penetration Testing**
Vulnerability Assessment shall be conducted to test the existing areas of exposure remaining which can be exploited by any threat. Penetration Testing needs to be conducted to test the withstanding capability of the protection provided to the application and networks. Most commonly one does VAPT for Network, Servers, Firewall, IDS to ensure that the IT infrastructure is free from any

vulnerability. Thereafter, corrective action should be taken for rectifying such vulnerabilities.

6. **ISMS Documentation**
   Several documentations including Business Continuity Plan needs to be maintained to fulfill the requirements of ISO 27001. The extent of documentation would depend upon the size of the organization, type of activities, scope of complexity of security requirements and system being managed. There are certain mandatory procedures to be maintained and followed such as:

   a) Management Review
   b) Internal Audit Review
   c) Control of Documents
   d) Control of Records
   e) Preventive Action
   f) Corrective Action
   g) Incident Management Response
   h) Effectiveness of Controls

7. **User Awareness and Training**
   ISMS is not only about documentation. The user should be aware of the information security for which appropriate training programmes needs to be conducted at regular intervals.

8. Preparation of Statement of Applicability
   A statement of applicability needs to be prepared which should include the control objectives and controls selected from the annexure A of the standard and the reasons for choosing the same; and map them to controls that are currently implemented; and exclusion of any controls along with justification for their exclusion. The statement of applicability provides a summary of decisions concerning risk treatment. Justifying exclusions provides a cross check that no controls have been inadvertently omitted.

9. **Audit**
   Organisations can go for a pre certification audit to determine the level of compliance vis-à-vis the standard. Thereafter, it can go for a certification audit.

The choice of certification body will vary from lines of business; to geography; to type of customers; characteristics, etc. Each certification body has their own certification life cycle. Generally it is 3 years with two surveillance audits per year. The certificate is valid for a period of three years and the organization has to go for recertification audit if they would like to renew or keep their certification in active status.

Conclusion:

How an organization can benefit from implementing / getting certified against ISO 27001:2005? How does it help in achieving security within an organization? This can happen through several steps described

1. The structured, measurable and controllable **security posture** is in place.
2. The stakeholders such as customers, suppliers, employees get a reasonable level of **assurance** on their security practices which means greater degree of reliance on their confidentiality (Privacy and sensitive information related), integrity (accuracy and completeness), availability (protection to critical and vital systems), and compliance to legal, contractual (SLA), and other regulatory requirements.
3. **Continual improvement** through structured monitoring and review of ISMS from internal and external audits.
4. This brings in a greater **competitive advantage** in business.
5. Reduction in **insurance premiums** over their regular and business continuity program. Prevent investments in unwanted areas.

Quiz 0002

a. Which programming languages are associated with buffer overrun?

b. Which of the following is a secure replacement for telnet?

c. What is a DoS attack?

d. Which network topology is often used to separate public services such as Web and mail servers from the internal network?

e. Which algorithms are used to compute digital signatures?

Terms & Conditions

- One Grand Prize winner will be awarded a cash prize of INR 1000.00.
- Three consolation prizes will be gift hamper of 3 books published by CRPCC/Sysman.
- Winners having all correct entries will be selected by lottery.
- If there is no "all corrrect" entries no prize will be awarded.
- Decision of CCCNews will be final and can not be challenged.
- Gift hampers will be collectable from CCC News office in Mumbai.
- Last date to send entries is 07 July 2009 IST 24:00 hrs.
- Winners will be declared in next issue of CCC News Magazine.
- Please send email with correct answers of all 4 questions to quiz@cccnews.in with your name, age, designation (if any), company (if any), Postal address, Phone no. & email address, please write "Quiz 0002 answers" in subject.
- Ambiguous answers may be out right rejected

Answers to Quiz 0001

a. Green Dam Youth Escort, Images
b. 38%
c. Maryland & Virginia
d. 2,50,000 $

The winners of Quiz 0001

Grand Prize
Mr. Srinivas Rao
Chennai

Consulotion Prize
Ms. Geeta Sinha
Delhi

Mr. Vijay Thangraj
Mumbai

Mr. Arjun Roy
Mumbai

All that is necessary for the triumph of evil is that good men do nothing

1. Pioneer in IT Security since 1991
2. Empanelled with CERT-In
3. Done over 2000 IT Security assignments
4. Provide Research Support
5. Create Public Awareness
6. Published 5 Books / 50 papers
7. An associate consultant to BSI to implement ISO 27001-ISMS

Sysman Computers Private Limited, Mumbai
sysman@sysman.in or +91-99672-47000