The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

1 May 2014

Purpose
Educate recipients of cyber events to aid in the protection of electronically stored corporate proprietary, DoD and/or Personally Identifiable Information from theft, compromise, espionage, and / or insider threat

Source
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
To receive this newsletter please send an email to scott.daughtry@dtra.mil

Disclaimer
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

NMCIWG Members
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, Sandia Labs

Distribution
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings Credit is given to the NMCIWG for the compilation of open source data

Security Experts Warn of Possible Russian Cyberattack against the U.S., Ukraine
Huffington Post, 30 Apr 2014: Former U.S. security officials warned on Tuesday that Russia may use cyber warfare against the U.S. and Ukraine if tensions between the two sides continue to escalate. "If we move to the heavy sanctions, the sectoral sanctions ... the Russians are going to strike back in some way," said former U.S. counterterrorism czar Richard Clarke, who spoke on a panel about cybersecurity at the Milken Institute Global Conference in Beverly Hills, California. "[Russians] can't strike back … [with] economic sanctions that would have the same kind of effect. What they can do … is a cyberattack to get back at us … attacking our financial institutions in ways that we'll never be able to prove it was them but we'll suffer the pain." Former Defense Secretary Leon Panetta, who also spoke on the panel, said the U.S. should work with Ukraine to prepare a defense against this potential cyberattack. "We've seen [Russia] use [cyber warfare] in Georgia. We've seen some elements of that being used in Crimea," Panetta said. "If [Russia] has an attack plan, a cyber element is very much a part of that attack plan. It takes down communications, takes down missile systems, takes down the counter attack…" Panetta went on to call cyberattacks the "battleground of the future," and said that Russia is second only to the U.S. in its cyber capability. "The sophistication of what's being developed today has the ability to create a lot of hell," Panetta said. "[Our] adversaries are looking at computer systems that run our electrical grid … chemical systems … water systems … transportation systems … financial systems." The three panelists noted that cyberattacks already frequently happen to U.S companies. Earlier this year, hackers stole the personal and financial data of 110 million Target shoppers, revealing the vulnerability of large companies' security systems. A study last year by the Ponemon Institute, a private security research group, looked at 60 companies across various sectors and found that they faced an average of two successful attacks each week, an 18 percent increase from the institute's study in 2012. To read more click **HERE**

April 29, Boston Globe – (Massachusetts) **Boston Medical Center fires vendor after data breach.** Boston Medical Center notified about 15,000 patients that that their personal records, including physicians' notes, were posted without password protection on MDF Transcription Services' Web site. The medical center discovered the breach March 4, had the Web site removed from the Internet, and fired the vendor and its subcontractors. Source: http://www.bostonglobe.com/business/2014/04/29/boston-medical-center-fires-vendor-after-data-breach/jboHN1Aq1x2JAE5amyEHiO/story.html

April 29, WFMZ 69 Allentown – (Pennsylvania) **Patients' medical billing records missing for 2 years.** Reading Health System notified former patients of Western Berks Internal Medicine April 29 that 3 boxes, containing 1,845 medical billing records were taken from the Spring Township practice in March 2012 and returned March 24, 2014. Authorities are investigating after the health system was notified when a maintenance service vendor told hospital officials he found the boxes at the practice's former office and took them home. Source: http://www.wfmz.com/news/news-regional-berks/patients-medical-billing-records-missing-for-2-years/25714310

Microsoft tells IE users how to defend against zero-day bug

C/NET, 30 Apr 2014: Microsoft has yet to patch its latest critical Internet Explorer zero-day security flaw, but an advisory about the bug now offers two temporary solutions. Updated on Monday, Microsoft Security Advisory 2963983 offers new information about the new zero-day vulnerability that affects all versions of Internet Explorer. The flaw could allow remote code execution and has already been used in "limited, targeted attacks," Microsoft revealed, though those attacks have so far affected only IE versions 9, 10, and 11. The potential reach of the bug could be widespread. Estimates of IE usage range from about 22 percent of people browsing the Web (StatCounter) to more than half of the desktop browser market (NetMarketShare). The vulnerability is so severe that even US and UK security agencies have cautioned people using IE for now. So what does Microsoft suggest for people who still need to use Internet Explorer? Turn on a feature called Enhanced Protected Mode. Introduced in IE 10, this mode adds an extra layer of protection by preventing malware attacks from infecting your system. Microsoft explains how to enable Enhanced Protected Mode (EPM) in the "suggested actions" section of its advisory. The steps are outlined as follows:

1.To enable EPM in IE 10 or 11, click the Tools menu and then click Internet options.
2.In the Internet Options window, click the Advanced tab.
3.Scroll down the list of options until you see the Security section.
4.Look for the option to Enable Enhanced Protected Mode and click its checkbox to turn it on.
5.If you're running IE 11 in a 64-bit version of Windows, you also need to click the checkbox to Enable 64-bit processes for Enhanced Protected Mode.
6.Restart IE to force the new setting to take effect.
EPM is saddled with a couple of limitations. The feature supports only IE 10 and 11 and only 64-bit versions of Windows. And some websites and add-ons won't work with EPM enabled.

How do you protect yourself if you're running an older version of IE or use a site that doesn't play nicely with EPM? You can unregister an associated IE DLL file called VGX.DLL. Microsoft explains how to unregister this file in the suggested actions section. Until Microsoft can patch this bug, the best option is to use an alternate browser such as Firefox or Google Chrome. To read more click **HERE**

April 30, Softpedia – (International) **4chan hacked, attacker mainly targeted moderator accounts.** The founder of 4chan stated April 30 that the popular bulletin board site was breached by attackers who leveraged a software vulnerability to gain administrator functions and steal moderator account names and credentials. The vulnerability used by the attackers was patched once 4chan became aware of it. Source: http://news.softpedia.com/news/4chan-Hacked-Attacker-Mainly-Targeted-Moderator-Accounts-439939.shtml

April 30, Softpedia – (International) **14 security issues addressed with the release of Firefox 29.** Mozilla released the latest version of it Firefox browser, Firefox 29, which closes 14 vulnerabilities, five of which were rated as critical. Source: http://news.softpedia.com/news/14-Security-Issues-Addressed-with-the-Release-of-Firefox-29-440043.shtml

April 29, Help Net Security – (International) **99 percent of Q1 mobile threats targeted Android.** F-Secure Labs released its latest Mobile Threat Report, which found that 99 percent of new mobile threats detected in the first quarter of 2014 targeted the Android mobile operating system, and that 277 new threat families were discovered during the time period, among other findings. Source: http://www.net-security.org/malware_news.php?id=2756

Irish Telecoms Company Eircom Targeted by Hackers

SoftPedia, 1 May 2014: Ireland-based telecommunications company Eircom was forced to shut down its email service on Wednesday after detecting unauthorized access to the system. "Yesterday, we detected an intrusion on the perimeter of our email service and in accordance with our security procedures and industry best practice, we took immediate steps to lock down our email service and eliminate any threat to our 350,000 eircom.net email users," the company noted in an alert published on the Eircom community forum. The Office of the Data Protection Commissioner and other relevant bodies have been notified of the breach. While there's no evidence that the attackers have gained access to other systems or to customer information, as a precaution, email users are being advised to change their passwords now and on a regular basis in the future. The company is still working on determining the origin of the breach. In an update posted around two hours ago, Eircom informed customers that webmail access had been restored. All the emails that didn't reach their destination due to the shutdown of the service should have been delivered by now. Users who have questions about the incident can contact the company via its Twitter account, via the online chat service, or by calling 1901. To read more click **HERE**

Kaspersky Finds Major 0-Day Flaw in Flash for Linux, Windows, Mac OS

SoftPedia, 1 May 2014: Kaspersky security experts have discovered that an Adobe Flash Player 0-day vulnerability was present on all the platforms currently running the software, namely Windows, Mac OS X, and Linux. All the vulnerabilities and other security issues are now treated a lot more seriously after the Heartbleed bug was discovered in OpenSSL, which is a vital component of the Internet infrastructure. Adobe's Flash player is also an integral part of the Internet and it's present on most of the major platforms out there, even if some are trying to shake this dependency. It raises eyebrows when people find a security issue in Flash, a problem that is not only potentially dangerous, but also ready to be exploited on any platform. "We received a sample of the first exploit on April 14, while a sample of the second came on April 16. The first exploit was initially recorded by KSN on April 9, when it was detected by a generic heuristic signature. There were numerous subsequent detections on April 14 and 16. In other words, we succeeded in detecting a previously unknown threat using heuristics." "According to KSN data, these exploits were stored as movie.swf and include.swf at an infected site. The only difference between the two pieces of malware is their shellcodes. It should be noted that the second exploit (include.swf) wasn't detected using the same heuristic signature as the first, because it contained a unique shellcode. Each exploit comes as an unpacked flash video file. The Action Script code inside was neither obfuscated nor encrypted," noted the Kaspersky security experts on securelist.com. In such situations, the vulnerabilities are sent to the company, in this case Adobe. After working on a fix for a few days, Adobe has released a patch for Flash on all platforms. The security issue was named CVE-2014-0515 and it seems that so far it has been used only against the Windows platform. This doesn't mean that Linux and Mac OS X were not vulnerable, just that so far it seems that people running on these systems have not been affected. The Adobe Flash Player is no longer actively developed for Linux, and it only receives small security updates like this one. If you notice a small Flash update on your Linux system, you now know what it's for. Adobe also recognized the contribution of Alexander Polyakov of Kaspersky Labs in finding this 0-day bug and in solving this pressing security issue. To read more click **HERE**

4 Vietnamese Men Suspected of Installing SMS Trojans on 100,000 Phones Arrested

SoftPedia, 1 May 2014: Four individuals have been arrested by Vietnamese police on suspicion of stealing close to $100,000 (€72,000) after installing mobile malware on the smartphones of more than 100,000 users. According to Tuoi Tre News, the suspects are Ha Xuan Tien, aged 23, Nguyen Van Tu, 25, Nguyen Duc Luc, 24, and Tran Ngoc Hai, 29. Three of them work for a company called Soloha Investment, Construction and Trade Co., while the fourth suspect is the administrator of a website called adrocket.vn. The suspects are said to have used websites like soundfest.com.vn and clickdi.com to distribute malicious mobile applications. Once installed on smartphones, the apps sent out SMS messages to premium rate numbers. For each message that was sent, the device's owner was charged with 15,000

Vietnam Dong ($0.70 / €0.51). The cybercriminals managed to earn VND 2.1 billion ($99,600 / €71,400) since late 2013 until the time of their arrest. SMS Trojans are not uncommon. Security experts say that this type of malware can help cybercriminals make a lot of money. However, this is the first scheme of this kind uncovered so far by authorities in Vietnam. The four men have been charged with using computer and telecommunications networks, the Internet or digital devices to appropriate property. To read more click HERE

UK National Crime Agency Report Warns of Increase in Cyber Threats

SoftPedia, 1 May 2014: The United Kingdom's National Crime Agency (NCA) has published the National Strategic Assessment of Serious and Organised Crime for 2014. The report covers child exploitation and abuse, the criminal use of firearms, drugs, economic crime, immigration crime and human trafficking, and cybercrime. British authorities seem to be aware of the fact that cybercrime will be increasingly problematic in the upcoming period. The report highlights five main types of cyber threats:

- large-scale harvesting of personal and business data for fraud against individuals and organizations;
- attacks whose goal is to delete, modify or steal data to gain competitive advantage, gain control of infrastructure, damage reputations, or undermine user confidence;
- disruption of access to systems with the aid of distributed denial-of-service (DDOS) attacks;
- the increasing use of the services offered on the cybercrime marketplaces by traditional crime groups;
- the increasing use of support services critical to the success of cyber-dependent crimes by other crime actors.

Of these five threats, only the first is likely to remain constant, the rest are either increasing or likely to increase in the next one to three years, according to the NCA's report. When it comes to cyber-dependent crimes carried out by traditional crime groups, the agency highlights the limited capacity and capability of law enforcement to respond. It also emphasizes the increasing gap between the capabilities of law enforcement and criminals. "Specialist service providers and bespoke toolkits are opening opportunities for those criminals who have limited technical competence. Different organised crime groups who share the use of key criminal technical and other infrastructures is a growing threat. Criminal online forums provide a market place for the trading of such services," the report reads. "Distributed Denial of Service (DDOS) protocols capable of launching powerful attacks against business critical systems are increasing in numbers. These tools, coupled with better understanding of the financial and reputational damage they can cause, are increasing the industry's perception of DDOS as a significant threat." The NCA says that it's currently difficult to estimate the costs of cybercrime, but the agency notes that it could "reasonably be assessed" at several billion pounds each year. Many recent studies conducted by third-party security companies have shown that the UK is among the most targeted countries in Europe. For instance, the Regional Advanced Threat Report (**link**) published by FireEye earlier this week shows that the largest number of malware infections have been spotted in the UK. Furthermore, the country takes the second place when it comes to the highest advanced persistent threat (APT) activity. The National Strategic Assessment of Serious and Organised Crime 2014 report is available on the NCA's website (**link**). To read more click **HERE**

Over Half of European Financial Organizations Are Worried About Risks Posed by Contractors

SoftPedia, 1 May 2014 Ovum has conducted a cyber security study on behalf of enterprise data security provider Vormetric. The European edition of the Insider Threat report is based on responses from IT decision makers at financial organizations in the UK, France and Germany. The figures show that 55% of respondents believe that third-party contractors pose the biggest risk. Privileged users, such as IT administrators and non-technical employees with access to

sensitive information, are seen as a major risk by 43% of those who took part in the study. Just over half of respondents believe that insider threats are more difficult to detect compared to last year. 45% of respondents say that this is a result of the increased use of cloud computing technology. "Enterprises grow their use of cloud computing to take advantage of the business flexibility and financial advantages it brings," said Daniele Catteddu, managing director EMEA for Cloud Security Alliance. "The research shows that they feel that there are additional security risks from this growth, and details how cloud providers can enhance their offerings to better meet enterprise security needs for offsetting insider threats." 76% of European financial services companies claim that they plan on spending more to address insider threats. The spending is mainly driven by concerns regarding compliance (45%), followed by protection of reputation and the implementation of best security practices. In addition to the European edition of its Insider Threat report, Vormetric has also published a report for Australia. As far as Australia is concerned, over 90% of organizations don't feel protected against insider threats. Half of the Australian respondents also believe that it's more difficult to detect insider threat than last year. However, only 48% plan on increasing spending in this area. When it comes to cloud resources, 68% are concerned about the lack of visibility into the security offered by the service provider, while 64% are concerned about third parties accessing their data. "As large-scale breaches, APTs, and Snowden-related discussions dominate the news cycle, it is clear that insider threats are among the most prominent IT security issues facing organisations today, a feeling which is reflected within the findings of our report," noted Ovum Research Director Andrew Kellett. "From the data, it's clear that organisations are also struggling with new technologies like cloud, mobile and big data as they seek to protect themselves from insider threats." The complete European edition of the Insider Threat report (**link**) is available on Vormetric's website. You can also check out the complete Australian edition (**link**). For a summary of the European report, click on the header image. To read more click **HERE**

Sales drop as corporate data breaches rise

Heise Security, 1 May 2014: Consumers avoid doing business with a breached organization at an alarming rate, according to a new study commissioned by Identity Finder, the results of which were revealed at Infosecurity Europe 2014. Financial and banking institutions, healthcare providers and retailers stand to have significantly increased expenses and lose up to one-third of its customer/patient base after a data breach:

- 33 percent of consumers will shop elsewhere if their retailer of choice is breached
- 30 percent of patients will find new healthcare provider if hospital/doctor's office is breached
- 24 percent of consumers will switch bank/credit card provider if institution is breached.

"A significant proportion of affected consumers discontinue or reduce their patronage post-breach," said Al Pascual, Senior Analyst of Security, Risk and Fraud at Javelin Strategy & Research. "That's real money lost in customer churn and reduced sales, and certainly demonstrates how the reputation of the organization hits the bottom line. It's noteworthy that about a third of people will go as far as to find a new doctor, if their provider is breached, as we all know healthcare services can be a big hassle to change." Target recently quantified the reputational damage and sales impact of their recent data breach and stated it resulted in significantly reduced revenue following the announcement on December 19, 2013. However, the fiscal impacts expanded well beyond sales. Target saw stock prices drop and estimates $61 million in expenses to investigate the breach, offer credit-monitoring services, increase call center staffing and procure legal services. Not only will revenue go down, but also expenses will go up. There is a great deal of data supporting a significant increase in post-breach expenses such as compliance, legal, and victim reparation costs. The research finds identity protection services alone are a common cost to each industry:

- 54 percent of healthcare providers offer victims protection
- 40 percent of financial/banking institutions offer victims protection
- 30 percent of retailers offer victims protection.

"Organizations must be more proactive in preventing a breach by understanding where a data leak can originate. By discovering and managing sensitive information at its source and not at the perimeter or after the fact, businesses can identify risk, change employee behavior, and justify where to spend security dollars," said Todd Feinman, CEO at Identity Finder. For risk assessments to be successful, businesses should proactively create an internal sensitive data management initiative tailored to each organization encompassing the following five critical steps:

- Sift through irrelevant data and discover sensitive information
- Classify information and assign accountability to clean and protect
- Secure and remediate unprotected files / remove at-risk data
- Centrally monitor policies, actions, and good behavior going forward
- Report compliance with policy and regulation

To read more click **HERE**

IT sec pros surprisingly cavalier about mobile security best practices

Heise Security, 1 May 2014: A flash poll conducted at Infosecurity Europe 2014 by Centrify Corporation has found that 94 per cent of IT security professionals use third party applications on their mobile devices for work, with 82 per cent using up to 10 apps. "Applications are now at the heart of corporate IT and have become a vital part of how employees get the job done whilst either in the office or on the move. Removing access to applications isn't an option - in fact it would create more problems than it would solve," says Darren Gross, EMEA Director, Centrify. "But the risk for organisations is that the more cloud-based or mobile apps employees interact with, the more they create islands of identity that become harder for IT to track and manage." "How do you authorise access for thousands of employees across multiple devices and platforms? Let alone de-provision them when they leave the company. Identity and access can often be overlooked, but unless enterprises can find a unified way to securely identify individuals, they risk their business coming to a shuddering halt," he added. The poll also revealed that of the 169 people surveyed, 7 per cent of security professionals do not believe it is their responsibility to protect corporate information held on their personal device. A further 8 per cent do not have a password or PIN enabled on the mobile device that they use for work purposes, potentially exposing organisations to risk. Surprisingly, despite repeated warnings about the risks posed by WiFi networks, 52 per cent of respondents said that they have accessed sensitive corporate information over unsecure networks at locations such as a coffee shop or airport. Gross concluded, "As the poll shows, the majority of employees are now leveraging more and more applications on their mobile devices. We are now seeing a greater need than ever for unified security identity across multiple devices and platforms, which is why we have created a full suite of solutions – not only to bring security awareness to the enterprise but also provide the best-in-class tools to reliably protect a firm's personal data and applications from identity-related risks and attacks." To read more click **HERE**

London warbiking reveals worrying state of Wi-Fi security

Heise Security, 1 May 2014: At Infosecurity Europe 2014, IT security company Sophos this week highlighted the worrying state of wireless security in the UK's capital city, when it sent security expert James Lyne and his computer-equipped bicycle onto the streets of London to test how safe homes, businesses, and even people on mobiles phones are from cyber criminals. Lyne, Global Head of Security Research at Sophos, went "warbiking" across the city to track down unsecure wireless networks and spotlight user behaviors that could be exploited by rogue hackers, and he discovered some alarming results: "Incredibly, conventional wireless network security is still a major concern, despite the security industry assuming such issues had been resolved years ago. Many would assume these methods are 'old hat' but it is still a very viable attack vector that demonstrates basic security best practice is not being adopted. " says Lyne. "As our London Warbiking exercise found, there are an astonishing number of businesses and home users

employing insecure, poorly implemented, or even defunct wireless security protocols. With our voracious hunger to be online at all times, this is leaving millions of people, companies and their valuable data open to attack." London was the latest stop on the "World of Warbiking" tour - a global research project targeting major cities across the globe. Conducted over two days around the streets of the capital, Lyne's warbiking exercise revealed that of 81,743 networks surveyed, some 29.5 percent were using either the known-broken Wireless Equivalent Privacy (WEP) algorithm, or no security encryption at all. A further 52 percent of networks were using Wi-Fi Protected Access (WPA) - a no longer recommended security algorithm. "Even within the security industry there are myths and misunderstanding about what the real risks are with wireless. Many argue that the unencrypted, intentionally open networks (the majority of the 29.5%) are 'OK' as they use a captive portal to register users. Unfortunately the standard user doesn't recognize that major brand XYZ wireless is not encrypted and that their information can be picked up by anyone with £30 piece of equipment available on Amazon," said Lyne. Just as worrying was many people's total disregard for basic security. "Our experiment found a disturbingly large number of people willing to connect to an open wireless network we created, without any idea of who owned it or whether it was trustworthy, Compounded by the growing number of devices that are permanently identifying themselves via technology like Bluetooth, this kind of behavior is increasingly putting everyone's valuable data at risk." Lyne continued: "This willingness to connect to any wireless network that professes to offer free wi-fi, without ensuring you have some kind of security measures in place, is like shouting your personal or company information out of the nearest window and being surprised when someone abuses it. With a few extra command line arguments, it would have been trivial to attack nearly everyone in our study." The open wireless network created during the London experiment also offered an insight into what people are connecting to when they are out and about. Social media sites such as Facebook and Twitter were high on the list of most requested pages, along with webmail access and news websites. But worryingly, it appears many people are also choosing to access websites and services that could prove even more attractive to cybercriminals: Despite the fact that this was an open network, once connected many people seemed happy to access online banking sites, even though they had no idea who was running the access point. Only a tiny minority (2 percent) actually took responsibility for their own security by using a Virtual Private Network (VPN) or forcing secure web standards. "Our test was conducted strictly within the confines of the law," explained Lyne, "but the cyber criminals won't have the same concerns, so our experiment shows why people need to be much more aware of the potential dangers of connecting to open wi-fi networks when they are out and about." Details about the methodology used and results so far from the World of Warbiking project - along with tips on how to be more secure – are available **here**. To read more click **HERE**

63% of orgs believe they can't stop data theft

Heise Security, 30 April 2014: Websense released the first report of the Ponemon Institute survey, "Exposing the Cybersecurity Cracks: A Global Perspective," which gives new insight into why cybercriminals have a foothold in the broader enterprise. The new survey of nearly 5,000 global IT security professionals reveals a deficit in enterprise security systems, a disconnect in how confidential data is valued and limited visibility into cybercriminal activity. Findings reveal a global consensus that security professionals need access to heightened threat intelligence and defenses:

- 57 percent of respondents do not think their organization is protected from advanced cyber attacks and 63 percent doubt they can stop the exfiltration of confidential information.
- Most respondents (69 percent) believe cybersecurity threats sometimes fall through the cracks of their companies' existing security systems.
- 44 percent of companies represented in this research experienced one or more substantial cyber attacks in the past year.
- 59 percent of companies do not have adequate intelligence or are unsure about attempted attacks and their impact. Further, 51 percent say their security solutions do not inform them about the root causes of an attack or they are unsure.

- According to respondents, there is a gap between data breach perception and reality – specifically regarding the potential revenue loss to their business. 80 percent of respondents say their company's leaders do not equate losing confidential data with a potential loss of revenue. This is in contrast to recent Ponemon Institute research, which indicates that data breaches have serious financial consequences for organizations. The average cost per lost or stolen record due to a data breach is $188 and the average cost of an organizational data breach is $5.4 million.
- 48 percent say their board-level executives have a sub-par understanding of security issues. However, we believe that cybersecurity awareness has most likely increased from that of a few years ago.
- Less than half of the respondents (41 percent) believe they have a good understanding about the threat landscape facing their company.
- Only 37 percent of respondents could say with certainty that their organization lost sensitive or confidential information as a result of a cyber attack.
- 35 percent of those who had lost sensitive or confidential information did not know exactly what data had been stolen.

"While there are significant differences among countries for specific questions (such as availability of cyber attack intelligence), the overall analysis indicates that a majority of security professionals do not feel adequately armed to defend their organizations from threats," said Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. "This challenge is further compounded by a perception that company leaders do not believe that data breaches will lead to loss of revenue. Our research has shown this is simply untrue." The report surveyed IT security practitioners with an average of 10 years' experience in the field from 15 countries: Australia, Brazil, Canada, China, France, Germany, Hong Kong, India, Italy, Mexico, the Netherlands, Singapore, Sweden, United Kingdom and the United States. In addition to the survey results, the report also includes conclusions drawn from the data and recommendations for addressing the exposed cracks in current cybersecurity measures. To read more click **HERE**