Cybercrime Monitor - EMEA

Monthly Search

Nicola Varney

March – April 2015

AIG EMEA Marketing Centre of Excellence
Business Information & Intelligence
58 Fenchurch Street
London
EC3M 4AB
MarketResearch.AnalyticsEuropeEnquiries@aig.com

CONTENTS

ARTICLES

INCIDENTS

CONSTRUCTION

FIRM'S £12,000 BILL AFTER PHONE HACKED

laura redpath
30 March 2015
The Press and Journal

A north-east business was left with a £12,000 bill after its telephone system was hacked.

Bosses at Premier Fixing Solutions and Construction have told of their frustration after illicit calls were made from their line.

Bill Young and Keith Scott said they first knew something was wrong when they tried to dial externally on March 8, but noticed the lines were dead.

Mr Young, 56, said he immediately called 2 Circles, the line provider for the building material supply firm.

He added: "They told us we couldn't dial up because a bar had been placed on the lines due to unusual activity.

"That was when we found we had a bill for £12,000 and we freaked as the highest bill we've had is £400 or £500 a month."

After further talks with the UK-based communications firm, the business partners discovered the hackers had been tapping into the company phones and making premium calls from Sunday, March 1.

However, Andy Reid, director of 2 Circles, said that, although he sympathised with Premier Fixings, it was up to the business owners to make sure the phones systems were locked down.

He added: "These types of hackers get access because people don't have passwords on their phones.

"You can't leave your door unlocked have a stranger break in and rack up a huge electricity bill and then expect the provider to pay up.

"We have not yet billed Premier Fixings in respect to the fraudulent calls as the matter is still under discussion with the network."

Mr Young claims neither he nor Mr Scott had been made aware of the protective security available until now.

He said: "It's so frustrating trying to get to the bottom of it."

But Mr Reid said he sent an e-mail to the firm in July detailing the available security products. He added: "We also send e-mails out to all clients just before Christmas and Easter as we feel customers are at the greatest risk during the holidays."

Mr Young has contacted the police about the matter.

A spokeswoman for the force confirmed the fraud team received a complaint but the investigation had now been passed on to Action Fraud, the UK's national centre for fraud and internet crime.

TRANSPORTATION, COMMUNICATIONS, ELECTRIC, GAS, AND SANITARY SERVICES

CYBER-ATTACKS ON BA CUSTOMER ACCOUNTS

30 March 2015
The Herald

HACKERS have accessed tens of thousands of British Airways frequent flier accounts.

The airline said no personal information has been viewed or stolen, and it has frozen affected accounts for the next day or so while it resolves the issue. It means top executive club fliers may not be able to use their air miles until the issue is resolved.

Airline chiefs said only a small proportion of its millions of customers are affected, and that their names, addresses, bank details and other personal information have not been accessed.

The company apologised to customers and said it expects to have the system back up and running in the next day or so. It is not known who is behind the hack, but it is believed it was carried out by an automated computer programme looking for chinks in the armour of the company's online security systems.

A British Airways spokesman said: "British Airways has become aware of some unauthorised activity in relation to a small number of frequent flyer executive club accounts.

"This appears to have been the result of a third party using information obtained elsewhere on the internet, via an automated process, to try to gain access to some accounts."

FINANCE, INSURANCE, AND REAL ESTATE

NEW SOPHISTICATED BANK CYBER SCAM UNVEILED

6 April 2015
CXOtoday.com

IBM has uncovered a sophisticated fraud scheme run by cyber criminals that uses a combination of phishing, malware and phone calls that the technology company says has stolen more than $1 million from large and medium-sized global companies.

The scheme, which IBM security researchers have dubbed "The Dyre Wolf," is small in comparison with more recent widespread online fraud schemes but represents a new level of sophistication. It makes use of a

variety of advanced technology tools and social engineering tactic including malware, phishing, and phone calls, to dupe medium and large companies.

According to IBM, this fraud scheme is being run a group of cyber criminals from Eastern Europe. In a typical attack on a corporate account, says the IBM unit, a victim logs into a corporate account on their bank's web site and they are presented with an error notice that invites them to call the bank about accessing the account. But the security researchers revealed that these hackers target companies that regularly do wire transfers. The gang sends spam email to employees of such companies, with email attachments carrying a variant of the malware known as Dyre. If an employee opens the attachment, the malware installs itself into as many systems as possible in company's network.

If installed, the malware waits until it recognizes that the user is navigating to a bank website and instantly creates a fake screen telling the user that the bank's site is having problems and to call a certain number. If users call that number, they get through to an English-speaking operator who already knows what bank the users think they are contacting. The operator then elicits the users' banking details and immediately starts a large wire transfer to take money out of the relevant account.

The use of a live phone operator is what makes the scheme unique, said Caleb Barlow, vice president of IBM Security. He told Reuters, "What's very different in this case, is we saw a pivot of the attackers to use a set of social engineering techniques that I think are unprecedented," said Barlow. "The focus on wire transfers of large sums of money really got our attention."

IBM did not release any details on which companies fell prey to the scheme or the location of the perpetrators.

Once the transfer is complete, the money is then quickly moved from bank to bank to evade detection. In one instance, IBM said, the gang hit the victim company with a denial of service attack - essentially bringing down their Web capabilities - so it would not discover the theft until much later.

International Business Machines Corp's security unit is recommending that companies make sure employees are trained in spotting phishing attacks - where emails or attachments can infect a computer - and to never provide banking credentials to anyone.

SERVICES

CHENNAI ENGINEER GETS 2-YEARS IN JAIL FOR HACKING, DATA THEFT

2 April 2015
Press Trust of India

Hyderabad, Apr 2 (PTI) A court here has sentenced a Chennai-based software professional to two years' rigorous imprisonment for hacking servers of a local firm and stealing confidential data.

The court had on March 31 found Prabhakar Sampath guilty under Section 66 of Information Technology Act. Apart from the jail term, the court also imposed a fine of Rs 10,000 on him.

Sampath was accused of hacking the servers of SIS Infotech Private Limited, a city-based company, Superintendent of Police (CID-cyber crimes) U Ramamohan said in a release today.

The company sells market research reports. Sampath, a B-Tech degree-holder wokring with an IT firm in Chennai, hacked the server online and downloaded confidential reports in 2008, the SP said.

"The accused was traced through technical investigation, and police seized a pen drive, computers systems from his house and workplace containing research reports," the release added. PTI VVK KRK PAL

DATA BREACH SUIT AGAINST GOOGLE IN UK TO MOVE AHEAD

Mikolo Ilas
30 March 2015
SNL Real Estate Securities Daily: North America Edition

Google Inc. lost its bid to dismiss a lawsuit accusing the company of breaching data privacy of U.K. computer users.

The Court of Appeal of England and Wales dismissed Google's petition to dismiss the lawsuit and followed an earlier English High Court decision to move forward with the case, according to a March 27 news release.

In the case, Google was accused of secretly tracking hundreds of Apple Inc. customers in the U.K. by circumventing Apple's security settings on the iPhone, iPad and Mac devices and unlawfully installing cookies in Apple's Safari Web browser to track browsing habits of users.

The recent decision opens the door to litigation by U.K. citizens who used Apple computers, iPhones and iPads between the summer of 2011 and the spring of 2012.

TWITCH: USERS ACCOUNT INFO MAY HAVE BEEN ACCESSED IN POSSIBLE HACKING INCIDENT

Erik Chandler
Distributed by Contify.com
25 March 2015
StockWatch

Amazon-owned popular video game streaming platform Twitch has said in a warning to its users on Monday that their account information could possibly have been accessed through unauthorized means.

Warning the users of a possible hacking incident, Twitch said in a brief post on Monday that it has reset users' passwords and stream keys, and has also disconnected accounts from Twitter and YouTube.

The warning message also informed the users that they will have to set up a new password when they log in to the Twitch service the next time.

Along with taking steps to accelerate the expiration of users' passwords and stream keys as a precautionary measure, Twitch has also asked users to change the similar passwords which they may be using for other sites as well.

Meanwhile, Twitch has not made any official disclosure of the estimated number of user accounts compromised in the possible hacking incident. The company has also not specified what personal information of the users has been compromised in the hack. Twitch has simply said in its brief post that the

hacking incident has apparently breached "user account information;" and that the company will contact the affected users directly.

PUBLIC ADMINISTRATION

ISLAMIST HACKERS SEIZE CONTROL OF DEFRA'S AIR-QUALITY WEBSITE

Damien Gayle
8 April 2015
The Guardian

Group calling itself Moroccan Islamic Union-Mail posts picture of Saddam Hussein and criticises Britain for its role in invasion of Iraq
Islamist hackers seized control of the government's official air-quality website to post a message criticising Britain for its role in the invasion of Iraq in 2003.

Visitors on Tuesday morning to the UK-Air website, part of the Department for Food, the Environment and Rural Affairs, were greeted with a black background with a a large portrait of the former Iraqi dictator Saddam Hussein.
Beneath it a message in broken English read: "It's time to remind the British government what you did with Saddam Hussein will not forget. And we are ready to sacrifice with everything, as not to give up Iraq and stay alert for the coming…"

Twitter users noticed the hack, claimed by a group calling itself the Moroccan Islamic Union-Mail, as early as 7am. By 8am the message had been removed and replaced with a holding page. Moroccan Islamic Union-Mail appears to style itself as an Islamist version of the Anonymous hacking group.

A Defra press officer told the Guardian that the department was "aware" of the hack but could provide no further details at that time.

The hacked page included a link to an Arabic-language Facebook page for the Moroccan Islamic Union-Mail. A banner picture on the page showed eight masked men posing in T-shirts bearing the acronym MIUM. A link on the page led to a webpage hosting an Anonymous-style montage video made of news reports on the hackers' exploits.
On the news feed, the group claimed responsibility for a separate hack of Zambia's state website, as well as posting anti-Israel messages and comments on Middle East politics.

The Anti-Defamation League, which documents and counters racism, has previously accused MIUM of hacking on behalf of the Islamic State terrorist group. MIUM hackers have targeted Jewish websites in the US during the recent conflict between Israel and Gaza, the ADL said in a blogpost, before turning their attention to US military-linked websites in response to the American-led air campaign against Isis which began in December.

British forces are also involved in the campaign against Isis militants in Iraq. The backbone of the terror group is formed of Sunni Islamists, but elements of Saddam's Baathist regime – which was backed by Iraq's Sunni minority – are also said to support the insurgency.

The UK was part of the US-led coalition that invaded Iraq in 2003, toppling Saddam after nearly 24 years in power. The UK's role in the Iraq war has previously been cited as a justification for terrorist attacks and threats against British nationals.

Mention of the Defra hack was first made on Twitter by Jim McQuaid at 7.05am. The UK-Air home page usually publishes pollution forecasts for the coming days and data on the latest pollution levels. Normal service had been restored to the UK-Air site by 8.24am.

HACKERS HIT ISRAELI WEBSITES AFTER ANONYMOUS THREATS

7 April 2015
Associated Press Newswires

JERUSALEM (AP) — Pro-Palestinian hackers disrupted Israeli websites on Tuesday, following threats from the Anonymous hacking collective that it would carry out an "electronic Holocaust," though Israeli cyber experts said the coordinated attacks caused little damage.

The hacking campaign, which has taken place every April 7 since 2013, is meant to be in protest of Israeli policies toward the Palestinians. In 2013, the hackers first waged the coordinated campaign, dubbed OpIsrael, on the eve of Israel's annual Holocaust remembrance day.

Israel's Computer Emergency Response Team, a civilian cyber security group, said Anonymous attacked a few dozen websites belonging to Israeli musicians and non-profit organizations on Tuesday. Anonymous had vowed it would topple Israeli government websites, banks and public institutions, though no major disruptions were reported.

The hackers replaced website home pages with photos of a Muslim holy site in Jerusalem and of militants holding the Islamic State militant flag, and posted a message signed by "AnonGhost."

"We are always here to punish you! Because we are the voice of Palestine and we will not remain silent!" the message read.

A video message by Anonymous said its campaign was responding to "crimes in the Palestinian territories," including last summer's Gaza war.

Israel's national cyber bureau said it distributed instructions to "relevant authorities" about boosting defense for websites ahead of the planned attack.

BCOM EXAM CANCELLED - RU PAPER LEAKED ON WHATSAPP

7 April 2015
The Times of India - Jaipur Edition

Rajasthan University on Monday cancelled BCom's first year examination for Economic Administration and Financial Management (EAFM) subject after its question paper was leaked and circulated through WhatsApp by unidentified persons. "The leaked paper and the original ones were identical. So, the examination had to be cancelled," acting vice-chancellor of RU, Hanuman Singh Bhati said. The university filed a complaint in the Gandhi Nagar police station against unidentified suspects. The exam was scheduled for Monday and the administration came to know about the leak just hours before the test. About 35,000 students were to take the exam at 227 centres in seven districts. A committee has been formed by RU to probe the matter. Prime facie reports said the paper was leaked on Whatsapp from hyper-sensitive centres either in Dausa or Bharatpur.

Bhanwar Lal, SHO Gandhi Nagar police station, said, "We are investigating the matter and seeking the help of cyber crime experts to trace the culprites." Once the varsities authorites decided to cancel the exam, the administration swung into action and faxed the orders to all centres. At some centres, the message reached late and students were already taking the test Question papers are dispatched to farflung centres like

Bharatpur, Alwar, Dholpur, Sikar two to three days in advance. Once the paper reaches a centre, it is the centre's responsibility to conduct the exams without hassles.

DATA-BREACH POLICEMAN GETS ABSOLUTE DISCHARGE

rebecca buchan1
1 April 2015
The Press and Journal

A policeman who searched his work computer database for restricted information about his sisters has been granted an absolute discharge.

During the course of one day, Keith Knowles accessed seven crime files while at work at Woodhill House in Aberdeen's Westburn Road.

The documents – relating to his siblings Lynn Robertson and Veronica Knowles – were viewed for only a matter of seconds each. Knowles accessed the information for his own "curiosity" rather than for policing purposes.

Yesterday, the award-winning officer appeared at Aberdeen Sheriff Court, where he was due to go on trial facing four charges of breaching the Data Protection Act.

However, Knowles admitted committing one offence and his not guilty pleas to the other charges were accepted by the Crown.

The court heard the 49-year-old had been concerned about his sisters after receiving information that they may have been victims of a crime.

Representing Knowles, advocate Gareth Jones said he had searched the Grampian Police CrimeFile system on July 6, 2012, to find out what was happening.

When he saw the record he realised they were not the victims of any crime – but were actually suspects of an alleged offence.

Mr Jones said that the information was not examined for any more than 10 seconds before the files were closed, and no attempt was made to disseminate what he had read.

Mr Jones asked Sheriff James Tierney to consider imposing an absolute discharge on his client and passed him four references written by senior colleagues in the force.

He told the court that Knowles, who joined Grampian Police in 1994, had previously received a medal for bravery for his part in apprehending armed robbers.

Sentencing the officer, Sheriff Tierney said: "This is an out-of-the-ordinary case. Despite a warning to the contrary from the computer you were accessing the information, allowing your curiosity to get the better of you, and as a consequence now face disciplinary procedures. I have read four references which all show that you have been and continue to be an excellent policeman and a credit to the police force."

Sheriff Tierney said he believed the public interest would be best served if Knowles was allowed to continue to serve in the force and as a result an absolute discharge was appropriate.

UNIVERSITIES NEED TO PLUG INTO THREAT OF CYBER-ATTACKS

Lucy Ward
31 March 2015
The Guardian

Desirable research plus students' personal and financial details make universities a juicy target for cyber-criminals. But are they doing anything about it?

In January last year, Queen Mary University of London came under attack. There was no physical violence or break-in: this was a cyber-assault by the online hacking collective Anonymous, which claimed to have stolen data, including students' personal details, from the university's servers in revenge for what it called "invasive" research sponsored by the Ministry of Defence.

The case is now the subject of an information commissioner's inquiry over alleged breaches of data protection rules, and Queen Mary says it has taken steps to "significantly mitigate" the risk of such a "one-off breach in security" happening again. But can universities really be sure they can protect themselves from cyber-attacks?

According to Professor Awais Rashid, director of Lancaster University's security research centre, the unique nature of universities makes it difficult. As well as teaching and research, most are now involved in commercial activity – from venue hire to privately funded research – but they can't be "shut down" in the way other businesses might.

Students come and go, bringing laptops and mobile devices; visitors pass through from across the globe; researchers link up with organisations worldwide. "In many companies, even their own staff can't access the network through a device that hasn't been vetted," says Rashid.

The combination of students' personal and financial details, confidential data such as medical records, and commercially desirable research – plus an intrinsic virtual (and cultural) openness – makes universities obvious targets for cyber-attacks. Virtual assailants range from identity or information thieves to disgruntled students. Once hacked, universities can be left with high financial losses and reputational damage.

But despite the value of the intellectual property they hold, vice-chancellors do not always take the issue of cybersecurity seriously enough, says Martyn Thomas, visiting professor of software engineering at the University of Oxford . "Anywhere where there is information of significant value, people will be trying to steal it," he says, "usually with enormous success."

"Thankfully, many universities have changed from the 'computer says no' attitude

Carsten Maple

However, even sophisticated monitoring systems are no guarantee of protection, he points out, as Sony Pictures found to its cost when sensitive emails about its top talent were exfiltrated and published online last year.

This year, the government reissued guidance for organisations known as " 10 Steps to Cyber Security ". It has also developed the Cyber Essentials scheme, which is aimed at helping businesses and other organisations protect themselves from attacks. Most universities have not yet taken those steps, says Thomas, who recalls one institution that took months to realise its system had been hijacked and was hosting a pornographic website.

But creating secure IT systems for "large heterogeneous organisations" like universities is not easy, says Professor Carsten Maple, director for cyber security research at Warwick University and vice-chair of the UK's council of professors and heads of computing. "Thankfully, many universities have changed from the 'computer says no' attitude to one of 'let us help you do what you need in a secure and managed way', he says.

IT security isn't a new problem for universities. In 1986, an attempt to resolve a minor accounting error in computer accounts at Lawrence Berkeley National Laboratory, California, uncovered a West German hacker spying on defence information for the Soviet Union.

Today, it is still the "huge processing power of universities that is potentially attractive to the criminal fraternity", says Dr Alastair Irons, chair of the British Computer Society's cybercrime special interest group. He has noticed an increase in "phishing" attacks, in which recipients are sent emails falsely purporting to be from university accounts.

"You can say, 'I am going to close things down, run the university system the way I run a bank'," says Irons. "But then, of course, you can't do all the things you want to do as a student or academic." However, cybersecurity should be taken seriously and dealt with at board level by universities, he adds – just as in any company with valuable data to protect. Universities, he says, can be reactive and fail to perceive the extent of threats.

The key for universities, as they try to balance openness and protection, is working out what information genuinely needs protecting and ensuring they target their efforts on that. Guidance from Universities UK published in 2013 emphasised the need to make informed assessments of legal, reputational and financial risks posed by information held, and then introduce "proportionate and appropriate controls that focus protections on high-risk information".

For the most sensitive data, such as NHS patient information, this involves separation of computer systems to isolate valuable information completely from the university's main network, or placing it behind firewalls.

Public sector organisations feel they have to cover their arse all the time

Ros Anderson

Hugh Boyes, cyber-security expert at the Institution of Engineering and Technology , says: "If you're working with sensitive or valuable research data, then it behoves the university to put in place a system to protect that data, and not just go for the cheapest system they can."

For the institution as a whole, the focus should be on better "cyberhygiene", he says. Everyone has to learn to back up data and to beware of phishing emails. "It's about targeting and training people to be a bit more savvy and not leave laptops on trains."

But according to Ross Anderson, professor of security engineering at the University of Cambridge , there is a danger of universities going overboard: lurching into panic mode at the slightest hacking attack and imposing needless and expensive controls. The appropriate way to deal with "threats" such as a minor hack by a disgruntled student is to have the confidence to ignore them, he says.

Yet, pressure from vested interests such as software companies, auditors and others can push universities into needless action. "Universities as public bodies are at risk of having to do completely unnecessary due diligence because of inappropriately risk-averse responses to entirely frivolous incidents," he says. "Public sector organisations feel they have to cover their arse all the time. The great majority of costs from cybercrime are from flapping around."

Like so many challenges raised by the internet, cybersecurity is less a finite goal than a process – and one of risk management rather than risk removal. The best things universities can do is ensure departments have the appropriate level of security, says Anderson. And where data is of critical sensitivity, it should be treated not only with top-level security but also with an ethical approach.

“It is not just a matter of compliance, but of ethics,” he says. “If you see university information security as being a subject like any information security, then you will screw up. You have got to understand the context, but this message is not getting across.”

HACKERS TARGET FREEDOM OF INFORMATION SITE

30 March 2015
The Irish Examiner

The Government has been forced to update its freedom of information website after a security breach.

The www.foi.gov.ie website was hacked last Tuesday, displaying the messages ‘Hacked by HolaKo' and ‘We are the best of the rest. Free Palestine #SaveGaza' on a white background.

The Department of Public Expenditure, which has responsibility for the site, said it took down the site after the hack in order to rectify the problem “as a matter of urgency”.

“This website was taken off air on the night of Tuesday 24 March when it was discovered that the site's homepage had been compromised,” said a spokesperson.

“The website was back up and running on Wednesday 25 March. The website has now been upgraded to prevent a recurrence.”

The spokesperson declined to comment on who was responsible for the cyber attack on the site, which usually holds information on the Freedom of Information process.

Earlier this month, the Dublin Rape Crisis centre website was also hacked, by a group claiming to represent the Islamic State.

The message ‘Hacked by Islamic State (ISIS), We Are Everywhere' appeared on the home page of the website.

Global security analysts are sceptical, however, of hacks' claims to be affiliated with the militant group.

“There are no indications that the individuals behind these latest hacks have any real connection to Isis,” said Evan Kohlmann of Flashpoint Intelligence.

“These defacements have taken place amid a spate of recent attacks where ordinary hackers have cynically used far-fetched references to ISIS as a means of attracting media attention.”

Meanwhile, Today FM's Twitter account was “compromised” last week — the feed sent out spam messages and tweets with an equine theme on Wednesday.

The station's account sent out bizarre tweets to people looking to “fall in LOVE & make sweet musik” and appealed to those “searchin 4 Ur SXC stallion”. Photos of horses were also sent out.

Today FM quickly deleted the content, and apologised to anyone who had received spam from its account.

“Apologies folks, it appears our Twitter account has been compromised. We're working on getting it sorted,” it said.

A short time later the station changed all passwords related to the account and was “back in business”.

GOVT WEBSITES OF TWO DEPARTMENTS SHUT DOWN

29 March 2015
Herald

PANJIM, March 29 -- Against the backdrop of government websites being hacked, the government has shut down two websites, which were recently targeted by unidentified hackers, to carry out a security audit and eliminate security vulnerability.

In reply to an unstarred question in the recently concluded budget session Chief Minister Laxmikant Parsekar said the two websites - Directorate of Accounts and Directorate of Fisheries - will undergo security audit shortly.

Parsekar said that a total of 13 websites were recently hacked. However, there is no mention of the hacking of the official website of Goa Raj Bhavan and Information & Publicity Department.

The departments named in the reply are Department of Sainik Welfare, Directorate of Accounts, Captain of Ports, Water Resources Department, Directorate of Food and Drugs Administration, Directorate of Printing, Press and Stationary, NRI Commission, Office of Labour Commissioner, Goa Dental College, State Central Library, Directorate of Agriculture, Directorate of Fisheries, and Directorate of Sports and Youth Affairs.

"Of these websites, those of Directorate of Accounts and Directorate of Fisheries are currently shut down as their security audit has not yet been performed and the same would be functional once the website audit is carried out and becomes free from vulnerability," the reply mentions.

Parsekar said 11 of the 13 websites have been cleared of vulnerability and re-deployed on the newly configured web server. Parsekar was replying to a question by Fatorda MLA Vijai Sardesai who asked about the number of government websites hacked and being restored.

CHILDREN'S DETAILS LOST AND SENT TO WRONG PLACE BY COUNCIL EMPLOYEES

24 March 2015
Derby Evening Telegraph

POLITICS: Council reveals details of lost documents

BY CHRIS MALLETT P: 01332 411999 E: chris.mallett@derbytelegraph.co.uk T: @ChrisMallettDT DERBY children's personal details have been lost and posted to the wrong address this year by city council staff.

But the authority says staff training has raised awareness of data protection issues, reducing the chances of the same thing happening in the future.

The Derby Telegraph reported in January that a leaked council e-mail revealed mistakes were being made with people's personal information, including medical records.

In it, senior councillor Baggy Shanker warned staff there had been "too many" information security incidents at the authority.

Following a Freedom of Information request, the council has now revealed details of how documents and devices have been lost or stolen in the 12 months to February.

In the first few weeks of this year, the council mistakenly disclosed children's personal information three times.

On January 14, an employee lost a notepad which contained details of cases; on January 27, "review notes" were posted to the wrong address; and on February 4, a report was delivered to the incorrect address.

Mr Shanker, cabinet member for governance and transformation, said he was seeing a definite improvement in the way staff are handling personal data.

He said: "With the raised awareness of individuals and additional training in recent months, from what I'm seeing there's a definite improvement. "People are more openly reporting where there has been a potential breach. We are getting more feedback because of the training. "This will put us in a better position in the months and years ahead because people are that much more conscious of what the procedures are, which is preventing it from happening.

"And where it does occur, they know to report it."

Laptops containing personal information were stolen or lost four times in the past year.

An employee accidentally left their laptop in a bank on November 27, and laptops were stolen from employees' cars on June 12, August 26, and December 2. The council said that its laptops are encrypted, which means messages are encoded in such a way that only authorised people can read them.

Other incidents included minutes of a review relating to a child being delivered to the wrong address on August 4. In the original e-mail, Mr Shanker said recent data breaches included copying colleagues into e-mails containing private and confidential data, including medical records.

In the Freedom of Information response, the council said there had, in fact, been no incidents like this where information was actually disclosed. A council statement on the matter said: "Each case is dealt with based on the circumstances surrounding the data handling error and the level of risk attributable to it.

"All staff are required to undertake mandatory data protection training.

"Where staff have been involved in a data handling issue, a check is undertaken to see when they undertook the training.

"Where necessary, further training and support is provided."

HACKER DISABLES MAINE.GOV WEBSITE FOR HOURS

By STEVE MISTLER Staff Writer
24 March 2015
Portland Press Herald

AUGUSTA -- The central Internet portal to Maine state government offices was disabled for about three hours Monday morning after it was attacked by someone claiming to be a Russian hacker.

The hacker, who uses the Twitter account Vikingdom2015, boasted of the attack with a tweet: "http://maine.gov will be down for a while. ENJOY."

The takedown disabled state agency websites and prevented users from accessing online services, such as registering motor vehicles, downloading tax forms or purchasing hunting and fishing licenses. In addition to disabling the Maine state website, the attacker also claimed responsibility Monday for bringing down the New Hampshire state website, and previously claimed to have taken down government websites in New Jersey, Oregon and Nebraska.

Maine.gov went down just before 9 a.m. and was back in service shortly after noon.

Alex Willette, spokesman for the Department of Administrative and Financial Services, which oversees the Office of Information Technology, said the site had been hit by an external attack known as denial-of-service. Such attacks disable websites by overloading servers with thousands of requests.

"Attacks to high-profile government websites are very common, and a thorough investigation is underway," Willette said. "The important thing to note is that this was in no way a security breach, and we currently have no evidence to suggest that any personal information has been compromised."

Willette described the attack as an "unfortunate inconvenience," but stressed that sensitive data on state agencies had not been compromised.

The attack came roughly six weeks after the head of the state Office of Information Technology, Jim Smith, warned of an "unprecedented increase" in cyberattacks against the state's network in testimony before the Legislature's budget-writing committee. Cyberattacks against government agencies and businesses have increased in sophistication and frequency nationwide, according to reports by the U.S. Government Accountability Office. The incidents vary in severity, from disruption in service or website availability, to breaches that can extract sensitive data.

Vikingdom2015 previously tweeted a "hit list" of 50 state government sites that would be subject to attack. Maine and New Hampshire were at the top of the list. Vikingdom2015's Twitter profile contains a link to the Russian Federation embassy in Washington, D.C., but it's unclear if the attacker is affiliated with the Russian government or a Russian national.

The Twitter feed includes posts in which the attacker boasts of taking down other government and business websites.

Paul VandenBussche, general manager of Information Resource of Maine, a private vendor that works with the state to oversee and manage parts of the state's website, did not respond to a request for comment.

According to the U.S. Computer Emergency Readiness Team, part of the Department of Homeland Security, denial-of-service attacks are designed to disable websites rather than hack them to extract data. According to the team, there is no effective way to prevent a denial- of-service attack, or a distributed denial-of-service attack, in which multiple computers and servers are used to strike a website.

Both types of attack have increased over the past several years, according to Internet security companies. A 2015 threat assessment report by the Internet security company McAfee Labs noted that denial-of-service interruptions made up 39 percent of all cyberattacks in the third quarter of 2014.

Such attacks have been used by small nation-states or terror organizations to cripple business and government websites. Financial institutions, whose customers depend on 24-hour, 365-day online service, are among the top targets. In some cases, attackers have tried to obtain ransom money in exchange for halting an attack.

Cybersecurity is also a concern for government agencies. Attacks involving federal government agencies jumped 35 percent between 2010 and 2013, from roughly 34,000 to about 46,000, according to a 2014 report by the Government Accountability Office.

Smith, the head of the state Office of Information Technology, told the Appropriations and Financial Affairs Committee on Feb. 10 that attacks against Maine's network are on the rise. He said that in one day in July 2014, there were 36,000 hostile attempts to infiltrate the state's file transfer infrastructure, which contains sensitive data.

In his report to the Legislature, Smith said that protecting the network "not only requires new security apparatus," but also new technicians.

The technology office now runs on a two-year budget of $303 million. It has requested $285 million for the next two fiscal years in the budget it presented to lawmakers in February.

The office serves as a vendor to other state departments, billing them for the technical support and website development it provides. Financial data shows that the technology budget requests are on the rise for some state agencies.

Willette said some agency technology budgets could be increasing because of the timing of upgrades, such as an overhaul of an agency's website. For example, the two-year budget request for the Department of Education shows a $2 million increase over its current technology expenditure. Steve Mistler can be contacted at 620- 7016 or at: smistler@pressherald.com Twitter: @stevemistler

GOVERNMENT REVEALS PLAN TO MAKE LONDON CYBER CAPITAL

Francesca Nyman
23 March 2015
Post Magazine

The UK government today (23 March) unveiled plans to make the London market the cyber risk management capital of the world in a report released in conjunction with broker Marsh.

The study entitled 'UK: Cyber Security: The Role of Insurance in Managing and Mitigating the Risk' was produced in conjunction with 13 London market insurers and follows the cyber summit chaired by Cabinet Office Minister Francis Maude MP in November last year.

It follows a survey that found a significant knowledge gap around cyber coverage among UK companies, with only half the firms interviewed being aware the cover existed. Outlining its expectations of UK companies,

the government said firms needed to view cyber not as an IT issue but a key commercial risk affecting all parts of its operations.

Effective risk management needs to include a board-level owner for cyber risk, a joined up recovery plan and the use of stress testing to confirm financial resilience against cyber threats, it added.

In a bid to encourage greater adoption of cyber cover among smaller firms, the thirteen participating insurers have agreed to include the government's Cyber Essentials accreditation certificate as part of their risk assessment for SMEs. In addition, Marsh is launching a new cyber product for SMEs which it claims will absorb the cost of Cyber Essentials certification for the majority of firms.

The government is encouraging other brokers to follow suit. The report also recommends that brokers provide firms with a cyber- assurance statement to give the board confidence in the completeness of their cover.

Along with increasing the take up of cyber insurance among UK corporates, thegovernment outlined a number of steps designed to establish the capital as a global cyber hub. Lloyd's has agreed to work with government body UK Trade and

Investment to promote the cyber capabilities of the London Insurance market.

Meanwhile, a new multi-disciplinary taskforce set up by City UK will bring together different sectors to discuss a joint UK cyber offering related to insurance for export.

The report does not address the creation of a pool to handle aggregation risk, although Marsh UK and Ireland CEO Mark Weil told journalists at a pre-launch press briefing that the topic had been “hotly debated” in the course of the enquiry.

Weil commented one obstacle is the lack of claims data available but many also feel that the private sector should attempt to address the risk itself, before looking to government for support.

“My personal view is that the industry should just get on with it. The capacity is there,” he said.

Asked whether the cyber opportunity could help to offset some of the adverse trends seen in the London Market Group's recently published London Matters, Weil said: “I've been in the London market and over time there's been net migration local markets. That doesn't mean London's dead. It means London needs to reinvent.”

London is a unique beacon for large complex risks and cyber is that kind of issue," he added. A senior government official said the report should be “an extra tool in the cyber toolkit”. “We hope this report will start to demonstrate that London can be a frontrunner in cyber risks” they added.

PAKISTAN CYBER FIRM HACKED COMPUTERS OF INDIAN BUREAUCRATS

Silky Malhotra
12 March 2015
Digit

India, March 12 -- A Pakistan based cyber security firm has been stealing crucial government and defence information from India, according to a recent report.

IT firm FireEye stated that Pakistan based Tranchulas cyber security firm, has been helping Pakistani government prepare for cyber warfare and has been sending malicious emails to Indian government officials. The firm used terms like 'Devyani Khobragade', 'Salary hike for government employees', and Sarabjit Singh' in the subject line to entice government officials to open these mails.

Once the attachment was opened, a malware would infect the computers and collect data and send it back to the attackers. The firm used a Pakistani based virtual service provider- VPSNOC, which leased US hosting services to control the attacks. FireEye has reported the information after a thorough two year long investigation.

However, the Indian government, is denying any suspicious activity or prior knowledge about these attacks. Dr. Gulshan Rai, director-general of the Indian Computer Emergency Response Team (ICERT) stated, "It is incorrect. We have only seen cases of website hacking. However, they hold only public data."

A senior officer from the Indian intelligence bureau has however agreed that they were under cyber threat. He said on condition of anonymity, "We have seen many such attacks targeting Indian government and defence establishments, but in cyber space it is very hard to ascertain the actual source."

Manish Gupta, senior vice president at FireEye said in a statement, "They are essentially penetrating Indian government accounts to find out what the Indian government is up to. They are also targeting defence organizations. Some of the things that could be important to them could be what kind of weapons does India have, where are these weapons deployed, how many people are deployed in these regions, what is the organization structure, are there any military exercises planned."

India has been trying to improve its cyber defence capabilities after the Snowden leaks about NSA surveillance. According to reports, Cyber attacks on Indian websites have increased by 40 percent in the last 2 years. The Indian government has taken measures to improve security and has launched its own secure servers earlier this month.

Source: ET

CYBER-CRIME CLAMPDOWN

7 March 2015
Evening Times

FIFTY-SEVEN people have been arrested in 25 separate operations in a major clampdown on cyber crime.

Operational activity took place across Scotland, England, and Wales and saw officers deployed from the NCA's National Cyber Crime Unit (NCCU) and police forces around the UK.

A 21-year-old man was arrested after an alleged attack on Police Scotland website.

STATISTICS AND FACTS

FINANCIAL INSTITUTIONS AND CHALLENGES OF CYBER CRIME

1 April 2015
All Africa

Apr 01, 2015 (The Guardian/All Africa Global Media via COMTEX) -- New voices may have been added to the global campaign against the growing threat of cyber crimes on financial institutions, even as experts have prescribed the adoption of asset-based approach as a foil to the menace.

According to experts, in a report from the Global Trade Review (GTR), the traditional all-in-one Information Technology (IT) approach is no longer working and financial institutions should instead, build IT systems tailored specifically to each asset class on their balance sheet, giving priority to the most lucrative ones.

In Nigeria, cases of cyber crime have become a state matter and assigned a weightier repercussion for offenders, as government moves to curb the activities of internet scammers, who give the country bad name, both locally and internationally. However, equally thriving currently is the electronic fraud, which a body- Nigeria Electronic Fraud Forum (NeFF), said if left unchecked, is capable of wiping out entire profit line of an individual bank, as well as send a wrong signal against the financial inclusion drive.

Cybercrime refers to any illegal activity through the computer as primary means, as well as any illegal activity that uses a computer for the storage of evidence. It include crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism.

This may have been partly the motivating force behind the Central Bank of Nigeria 's intensified efforts to give the financial system a facelift through the Bank Verification Number project, which among other things, would foil identity theft and duplication of identities in various financial institutions.

The debit and credit cards used in the electronic payments system have as well undergone several reforms, policies and security "beef-up", in an effort to stem the growing tide of electronic-fraud in the country, which is however, a global issue. Already, the total loss made by Nigeria's Deposit Money Banks (DMBs) due to fraud related cases have been put at about N203 billion in the last 14 years, a development, which still persists in the industry with sophistication and some cases left unreported by some financial institutions.

But the stakeholders- NeFF, Nigeria Interbank Settlement System (NIBSS) and DMBs, appear more worried as the fraudsters become more ingenious in an effort to undermine every security measures put in place, duping unsuspecting customers of banks and corporate organisations of billions of naira.

The Director of Banking and Payment System, Central Bank of Nigeria (CBN) and Chairman of Nigeria Electronic Fraud Forum (NeFF), Dipo Fatokun, decried the number and size of frauds against organisations, which are on the rise. Fatokun, at NeFF's first general meeting of the year, with the theme: "e-Fraud: Shining a Light on Insider Abuse," Fatokun, said that recent investigations have revealed that as many as 20 or 30 persons are involved. "You need to take a non-traditional approach.

Unfortunately we're getting all these breaches because everybody is still persevering with the traditional route, which is not actually looking at the balance sheet, the key assets and trying to understand which IT infrastructure you have to support the operation that creates wealth.

You've got to tailor your defenses according to that, and it's not happening," the Group Director of cyber security firm, MWR InfoSecurity, Alex Fidgen, said. He noted that geopolitical monitoring could be an important part of cyber protection, as attacks are often socio-politically motivated, targeting organisations that support either publicly or in private certain government policies.

Specifically, he cited the virus allegedly used by Iran on Saudi Aramco in 2012, which wiped most of the company's computers and forced it to shut down its internal communication system and was seen by many as retaliation against Stuxnet, the computer virus used by the United States and Israel to destroy centrifuges in an Iranian nuclear facility in 2010.

Fidgen said the same attack is now "consistently poking and prodding the U.S. bank network" with small-scale attacks, and other countries have been looking at financial markets as an increasingly relevant target to hurt political adversaries.

"Your chief executives or senior board members expressing political views - that makes you a target. It brings the question: is geopolitical tension being measured properly in your organisation as a form of indicator to your likelihood of being attacked? Hardly anybody does that," he added. According to Fidgen, nation-states wanting to remain anonymous now give highly-organised criminal groups the remit to "do the dirty work for them", leading to a crossover between the capabilities of the criminal organisation and the government, and making it very difficult for defensive intelligence agencies to understand attacks.

Another important aspect of cyber protection is communication, which the Vice-President of a security outfit, Luke Beeson, explained that the forces of criminal hackings on an organisation lie in their ability and desire to share information, while commercial organisations generally limit communication with their peers, perhaps for fear of competition.

Regulators at a national level are poised to become increasingly involved in financial institutions' cyber security programmes- the perfect example being the Bank of England's CBEST Vulnerability Testing Framework, which aims to protect the UK's financial stability by implementing a cyber attack testing system in each of its financial institutions.

Fidgen added: "With CBEST, the Bank of England has done something absolutely superb. The UK recognises what's happening, and the financial industry needs to be defensively well organised for the future. As a nation, we now have a financial regulator directly assigned to investigate cyber attacks.

"They're not interested in you as an individual organisation - what they're really interested in is whether you would have a role to play in a systemic collapse. With this scheme you will start to see this kind of cyber security structure cascade through all the regulators." The Executive Director of Operations, First City

Monument Bank , Nath Ude, said that the consequence of the menace on the banking landscape has been reputational damage, loss of share value, loss of customer confidence and increased audit costs.

While citing NIBSS reports on the loss of revenue to fraudsters, he noted that between 2000 to the first quarter of 2013, banks had already lost N159 billion, and subsequently lost N40 billion for the rest of the year, while from January to September 2014, N4 billion more was lost. According to him, fraudulent activities are on the increase, which amount to severe consequences for the financial industry in Nigeria, even as most electronic fraud in recent times assumed the insider abuse dimension, including "dedicated employees."

He said banks could curb insider abuse by watching out for warning signs like employees living above their means, frequent manipulation of data by employees and continuous, excessive use and abuse of privileged and systems account.

"Banks will be able to combat electronic fraud by filtering out predatory employees, reviewing upwards, the required reliability status for all staff who need privileged roles to work as well as deploying appropriate prevention and detection technologies like CCTV monitoring and access cards with authorizations," Ude explained.

The Chief Internal Auditor, First Bank of Nigeria Plc , Uduak Udoh, pointed out that the fraud committed by an insider is always hard to detect than those by outsiders, as the impact is usually higher when an insider is involved. According to him, though, at a particular period, investigations showed that outsider fraud volume was 5,173, representing 99.79 per cent, worth N786 million, the insider related fraud volume was 11 (0.21 per cent) but valued at N114 million. "Outsiders and insiders remain the greatest challenge as they are both vectors and actors in e-fraud space.

For without them banks will have good sleeps and less rough relationships with customers and regulators. The outsiders are those outside the wall of the bank who wants to reap where they never sowed. They are social engineers, impostors, con artist and gold diggers. Outsiders are usually the first focus to protect against by banks," he said.

On the risk mitigation, FBN chief auditor said that each organization has to decide how much loss they are willing to tolerate, as each of these areas requires an investment, in some cases substantial investments that may outweigh the benefits. "Even with these controls in place, there will still be the residual risk of user carelessness or of those angry users who are determined to circumvent the system. Thoughtful implementation of some or all of these controls can deter, prevent, detect, or reduce the ultimate impact of the incident," he suggested.

However, as part of efforts to stem the tide of the menace, Fatokun, NeFF chairman, said the forum has created an avenue for information exchange and knowledge sharing on fraud issues among key stakeholders to foster collaborative and proactive approach in tackling the challenge and limiting occurrences, as well as losses.

The forum has reiterated the need to collaborate more, think ahead and creatively too, to successfully tackle the fraudulent activities, which have been assessed as increasingly devising sophisticated techniques in approach.

The Head, Information System Security, NIBSS, Olufemi Fadairo, decried that 2014 was quite alarming in terms of fraud as it recorded very high volume of fraudulent transactions, noting that the unreported cases were far higher than the reported cases of frauds perpetuated in the system. Fadairo pointed out that Internet and ATMs remain the most popular channels for e-fraud, with Point of Sales (PoS) terminals being the preferred channel of cash out for fraudsters.

According to him, in 2014 there was a record of 1,461 fraud cases, with attempted value of N7.8 billion and actual loss value of N6.216 billion; in 2013, the fraud cases were 855, with attempted value of N19.149 billion, while actual loss value was N485.194 million, but added that the fraudulent cases emphasize the need for more security measures in handling payment cards on individual level and improved security practices as corporate bodies, to minimize fraud rates.

UAE ANDROID USERS FAILING TO PROTECT AGAINST MOBILE THREATS

ArabianBusiness.com Staff
29 March 2015
ITP.net

Lack of awareness of security threats to mobile devices is causing many Android users in the UAE to leave their handsets unprotected, according to a survey by Kaspersky Lab.

The survey found that 29% of Google Android users in the UAEw ere not aware of the existence of cyber threats targeting mobiles. Only 51% of Android-based smartphones and 56% of Android tablets are protected by an anti-virus solution, while 25% of smartphones and 31% of tablets are not even password-protected.

Globally, 18% of unprotected Android-based smartphones contain precisely the information that attackers are most eager to find: PIN codes for bank cards, passwords to online banking systems and other financial data. Twenty-four per cent of them store passwords to social networks, personal and work e-mail, VPN and other sensitive resources. Even though users can't be bothered to set a password to stop unauthorized access to their devices, they still store personal emails (49%), work emails (18%), as well as the "data that they would not want anyone to see" (10%) on their smartphones.

Furthermore, Android users encounter online threats more often than the users of Windows-based devices. The latter also know more about the dangers and tend to protect their devices in 9 out of 10 cases. Thus the survey found that over a 12-month period, 41% of smartphone users and 36% of tablet users faced malicious applications, 18% of smartphone users and 24% of tablet users had their online service accounts hacked, while financial cyberattacks affected 43% of smartphone users and 50% of tablet users. The average figures for all devices based on different platforms accounted for 31%(malicious applications), 14% (hacking online service accounts) and 43% (financial cyberattacks) - significantly lower than the Android-only figures.

"It is not surprising that mobile users are facing online threats more often now: devices are capable of doing so much more, and many more people are using them, so of course they will attract fraudsters. To avoid falling victim to scams, users are advised to protect their devices against cyber threats and be especially careful with any sensitive data stored on them," said Victor Yablokov, Head of Mobile Product Line at Kaspersky Lab.

CYBER-ATTACKS WIDESPREAD IN THE UAE, STUDY FINDS

ArabianBusiness.com Staff
25 March 2015
ITP.net

The majority of information technology decision makers in the UAE believe that their organizations were victims of cyber-attacks in the last 12 months, and almost all of them expect to be targeted again in 2015, a recent survey commissioned by security firm Bit9+Carbon Black showed.

About 86 per cent of organizations polledby Vanson Bourne, an independent specialist in market research for thetechnology sector, suspect that their systems were breached in 2014, with 96per cent of them saying that they could be likely targeted again at any pointover the next 12 months. All respondents have either full or partialresponsibility for their organizations' IT security, and are with organizationshaving at least 500 employees.

A variety of attackers launch their assaultfor diverse reasons, but the respondents expect that their organizations aremore likely to be targeted by corporate competitors (45 per cent); be attackedin order to be sabotaged (33 per cent); and have their intellectual property(IP) stolen (36 per cent).

Only a small portion of those polled,however, showed confidence in the ability of their systems to fight offpossible online threats. The survey results revealed that only seven per centof the respondents are completely confident in their companies' anti-virussolutions, while only five per cent rate their organizations' detectionabilities as excellent.

The results further disclosed slow responsetimes to online breaches. Most respondents (71 per cent) report that it takesmore than 30 minutes to identify where malware has been introduced into the ITenvironment, while many of them (72 per cent) say it takes more than 30 minutesto respond to a malware incident.

When asked what aspects of theirorganizations are the most vulnerable to cyber-attacks, the respondentsperceive mobile devices (31 per cent) and infrastructure servers (24 per cent)as the most susceptible.

Harry Sverdlove, Chief Technology Officerof Bit9+Carbon Black, said: The survey clearly demonstrates that mostorganizations are being targeted, hence the need to consistently enhance andimprove their information security. Cyber-attacks hit companies of all typesand sizes, often resulting in the theft of confidential information,substantial financial losses, and damaged reputations. Traditional endpointsecurity solutions, such as anti-virus, are insufficient against today'sadvanced threats and targeted attacks.Bit9 + Carbon Black is focused on providing our customers a new-generationof comprehensive endpoint security solutions to effectively prevent, detect andrespond to the increasingly sophisticated and relentless attacks facingorganizations."

Bit9+Carbon Black commissioned the surveyto shine a light on the cyber threat mindset of organizations in the region andhelp companies determine if they have the best endpoint security solution inplace to protect their information, including customer data, from theft ordestruction.

The study aims to provide a better understandingof the benefits of adapting powerful detection and response cyber securitysolutions for IT decision makers, CEOs, managing directors and enterpriseowners. It also has the objective of helping understand the involvement of therespondents in huge projects such as 'Smart City' and 'Smart Government,' andhow crucial it is to have a proficient cyber security system to protectenterprises from costly attacks.

WHAT IS THE TRUE COST OF A DATA BREACH TO AN ORGANIZATION?

24 March 2015
Emirates News Agency (WAM)

(GlobeNewswire) - Data breaches are increasingly impacting businesses across the globe, with the average cost paid by a breached organization reaching $5.9 million at the end of 2014. To provide a resource for payments industry stakeholders to understand the true impact a data breach might have on their organization, the Smart Card Alliance released today a new white paper, "The True Cost of Data Breaches in the Payments Industry."

The white paper, developed by the Smart Card Alliance Payments Council, helps issuers, merchants, acquirers and processors to analyze and understand the potential costs of a data breach and create the business case for developing a proactive data breach prevention strategy and for creating breach response plans. The white paper can be downloaded at http://www.smartcardalliance.org/publications-the-true-cost-of-data-breaches-in-the-payments-industry/.

"This white paper provides a resource for organizations to better understand the substantial tangible and intangible costs associated with data breaches, and why investing in strong preventive technologies is important," said Randy Vanderhoof, executive director of the Smart Card Alliance. "The impact of a data breach reaches all levels of an organization. Therefore, an upfront, preventative approach, such as layering EMV chip technology, tokenization and encryption, is an effective way to prevent breaches and reduce costs if a breach does occur."

The white paper addresses these key topics:

Definition of a data breach, clarifying how breaches can occur and what is considered a data breach

Recent data breach statistics and reported costs

Definition of both quantifiable and intangible costs that need to be considered when calculating the total cost of a data breach. Some of the potential costs include card reissuance, chargebacks, credit monitoring, fraud analysis, legal fees, liability costs, loss of "top of wallet" status, lost revenue, penalties, security upgrades and others

Identification of the impact for different costs for each stakeholder group, including acquirers, merchants, issuers, card holders, payment brands and others

For more resources from the Smart Card Alliance Payments Council, visit http://www.smartcardalliance.org/activities-councils-payments/.

More information on securing payments infrastructure with EMV chip technology, tokenization and encryption can be found in another Payments Council white paper, "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," available for download at http://www.emv-connection.com/technologies-for-payment-fraud-prevention-emv-encryption-and-tokenization/.

White Paper Contributors

Participants involved in the development and review of "The True Cost of Data Breaches in the Payments Industry" included: ABnote, American Express, Capgemini, CH2M HILL, CPI Card Group, First Data, Fiserv, Giesecke & Devrient, Heartland Payment Systems, Infineon Technologies, Ingenico, INSIDE Secure, Intelcav, NXP Semiconductors, OATH, Oberthur Technologies, OTI America, Tyfone, Verifone, Visa Inc.

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology.

Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

Michael Smith
Montner Tech PR
203-226-9290

For the original version on GlobeNewswire visit: http://globenewswire.com/news-release/2015/03/24/718130/10126019/en/What-is-the-True-Cost-of-a-Data-Breach-to-an-Organization.html

LEGISLATION, GOVERNMENT INITIATIVES AND POLICY

BELGIAN ARMY'S DEFENCE STRATEGY TO INCLUDE CYBER SECURITY

7 April 2015
Xinhua News Agency

BRUSSELS, April 7 (Xinhua) -- The Belgian armed forces are set to add cyber security to its defence strategy from 2019, local media reported on Tuesday.

In addition to its current operational capabilities, the Belgian armed forces plan to engage in a program of cyber security that includes detection and prevention of attacks from outside, as well as carrying out cyber attacks of its own, De Standaard reported.

In an interview with De Standaard, Lt. Col. Miguel De Bruycker, head of Cyber Defence at the General Intelligence and Security Service, said that "if counter parties intrude on our systems, they can steal information, delete or falsify data and interfere with normal operations. We must ensure that does not happen."

The new cyber security arrangements will be in operation from 2019.

According to Miguel De Bruycker, the aim of the arrangements is to discourage countries, organisations and individuals from launching a cyber attack on Belgium, as well as giving the defence forces the skill to launch their own counter attack.

"We sometimes have no choice but to proceed experimentally. Our techniques are constantly being refined," he said.

The priority of military cyber security is the protection of defence communications and information, as well as its weapon systems.

"Our service is operational at all times. In fact, it is constantly at war," said Miguel De Bruycker.

Enditem

UK GOVERNMENT ANNOUNCES £5M ANTI-MALWARE FUNDING

Alastair Stevenson
24 March 2015
V3

Funding to help create anti-hacking research centre at Queen's University Belfast

The UK government has announced a £5m investment to help researchers create new cyber security solutions as part of ongoing efforts to bolster the nation's defences.

The funding was announced at the World Cyber Security Technology Research Summit in Northern Ireland and will be provided by the Engineering and Physical Sciences Research Council (EPSRC) and Innovate UK.

It will be used to fund research and to help develop a Centre for Secure Information Technology (CSIT) at Queen's University Belfast.

The research will focus specifically on ways to tackle malware threats, detect intrusions and prevent data theft on laptops, smartphones and cloud storage services.

The CSIT is one of seven UK Innovation and Knowledge Centres being funded by EPSRC.

EPSRC invested £7.5m to create centres at Oxford University and Royal Holloway, University of London in 2013.

Professor John McCanny from CSIT said that the centre will offer students unparalleled training and help plug the widely reported 'cyber skills gap'.

"This further investment in CSIT recognises how over the last five years we have successfully blended world class research and innovation to deliver economic impact nationally, internationally and regionally," he said.

"This funding will allow us to further accelerate new value creation in this sector, drive business venture creation through our new pre-accelerator programme and build capacity for the industry by providing it with high calibre Masters and PhDs graduates."

Kevin Baughan, director of technology and innovation at Innovate UK, mirrored McCanny's sentiment and said he expects the centres to help plug the gap.

"CSIT has delivered significant UK economic growth through our original joint investment with EPSRC, contributing to over 950 new jobs in the Belfast cyber security cluster," he said.

"By extending funding for a further five years, we underline our support for their commitment to raise the commercialisation bar even higher. This will help companies of all sizes grow through leveraging the excellent UK science base in cyber security."

The news follows widespread reports that the UK is suffering a shortage of skilled security professionals. Julian David, chief executive at TechUK, listed the shortage as one of the biggest problems facing the UK technology industry.

EPSRC is one of many powers investing in university cyber security initiatives. The GCHQ-backed cyber security courses at six universities were approved in August to help tackle the skills gap.

INSURANCE

CYBER ESSENTIALS: PRACTICALITIES FOR BROKERS

Jack Elliott-Frey
31 March 2015
Insurance Age

Jack Elliott-Frey of brokers Safeonline shares tips for brokers on cyber insurance.

The past month has been a busy one for insurance brokers operating in the cyber risk class, due to the launch of a joint initiative by the Government and the insurance sector to help cement the UK's position as the global leader in cyber security insurance.

This new initiative builds on the 10 Steps to Cyber Security guidance published in late 2014, and the Cyber Essentials Scheme which is designed to encourage basic cyber security practice within businesses.

One of the key points that stands out from an insurance broker's perspective is the recommendation that participating insurers include Cyber Essentials (CE) accreditation as part of their risk assessment for SMEs. Marsh has outlined plans to launch a cyber product for SMEs to do this, and absorb the cost of CE certification, which the government encourages other insurance brokers to follow.

Reality

But what is the reality for brokers who may be deciding whether to offer CE certification as part of an insurance solution?

Brokers should offer up a ‘cyber assurance' statement themselves, to let clients know that they have implemented best practice and have the knowledge required to deliver complex, technical cyber solutions.

Many businesses are in the dark about this risk - brokers need to assure clients that they are not.

Although a cyber insurance policy may absorb the cost of CE accreditation, this should not be the key reason for choosing to utilise a specific insurance solution or underwriter.

The client and broker need to carefully consider the exclusions within the policy; For example some cyber policies don't cover terrorism if it comes in the form of a cyber attack, and so it is crucial to know what is covered and what is not.

Understand what it is you want to achieve by offering CE certification as part of a product. Are you trying to target a certain industry sector i.e. healthcare, manufacturing or retail?

If so, there are varying regulations that apply, as well as certain insurance markets that will or won't write cyber (depending on the sector); so ensure your product targets a sector where there is sufficient underwriting appetite.

Consider what the product will be covering aside from the cost of CE accreditation. There are numerous types of cyber risk, from cyber extortion through to physical asset damage and business interruption. The coverage is only going to broaden as this Cyber Essential initiative encourages the market to widen the scope of cyber insurance to cover other forms of attack. Much like exclusions, terms of coverage will be equally important when creating an attractive product.

Finally, the most important aspect of any product: price. Cyber policies are considered to be relatively expensive.

This is due to the complex nature of the risk as many insurers don't understand how to effectively price their offering. Brokers need to have a proper, thorough understanding of the risk your product covers and clients/insurers alike will respect this and be able to price accordingly.

Jack Elliott-Frey is a broker at cyber insurance experts Safeonline.

AGCS APPOINT FIRST DEDICATED CYBER RISK CONSULTANT IN THE UK

30 March 2015
Kuwait News Agency (Kuna)

Allianz Global Corporate & Specialty (AGCS) has appointed Rishi Baviskar as Cyber Risk Consultant, an expanding area for the AGCS's global risk consulting team. He will report to Dennis Murphy, AGCS Risk Consulting Regional Manager and work alongside the AGCS Head of Fidelity, Nigel Pearson. Based in London Rishi will support clients globally.

Rishi has over 15 years' experience working within the IT field for large oil, gas, automotive and pharmaceutical companies. In his previous roles, he has worked across all levels of process development ranging from onsite engineer to the design and implementation of cyber security policies. He is an industry expert in cyber security and the industrial controls required to create secure IT platforms.

Dennis Murphy, AGCS Risk Consulting Regional Manager said:

"In our recent annual risk survey, cyber was picked up as a growing concern rising 3 places to 5th in 2015. To continue to offer the best service, and address this concern, we have taken the step to appoint Rishi who will be solely focussed on working with our clients in this area. His wealth of knowledge and industry experience will be a great benefit and enhance our overall offering.''

Rishi added: "AGCS is extending their risk consulting services for cyber risks, a clear sign of their commitment. During my time in the industry, I have seen cyber-attacks increase significantly and the challenge of combatting them. My role will be to share my knowledge, work with clients to offer solutions and ensure they are fully operational as quickly as possible should a cyber-incident take place.''

AGCS HIRES FIRST UK-BASED CYBER RISK CONSULTANT

Katie Marriner
30 March 2015
Post Magazine

Allianz Global Corporate and Specialty has appointed Rishi Baviskar as its first UK-based cyber risk consultant.

Baviskar, pictured, has more than 15 years' experience working within IT for oil and gas, automotive and pharmaceutical companies. At AGCS he will manage global clients.

Dennis Murphy, AGCS risk consulting regional manager, said: "In our recent annual risk survey, cyber was picked up as a growing concern rising three places to 5th in 2015. [Baviskar's] wealth of knowledge and industry experience will be a great benefit and enhance our overall offering.''

Baviskar added: "During my time in the industry, I have seen cyber-attacks increase significantly and the challenge of combatting them. My role will be to share my knowledge, work with clients to offer solutions and ensure they are fully operational as quickly as possible should a cyber-incident take place.''

CYBER VETERAN MILNER JOINS MILLER

Andrew Tjaardstra
30 March 2015
Post Magazine

Simon Milner has joined global broker Miller to help grow its cyber book.

Miller wants to grow its position in cyber as its sees rising demand for the product globally.

Milner, pictured, has been broking cyber risks since 1997 and was most recently a partner at Jardine Lloyd Thompson.

He will work alongside Nick Fearon and the Miller team in London.

CONGRESS SEEKS SOLUTIONS ON CYBER RISK; INSURANCE SEEN AS KEY TOOL TO BOLSTER SECURITY

MARK A. HOFMANN
30 March 2015
Business Insurance

Following a year of several widespread cyber breach incidents, Congress is poised to encourage the insurance industry to take a lead role in bolstering cyber security.

That was evident earlier this month as the Senate Commerce Committee's Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security held the first congressional hearing on cyber insurance.

As the panel's chairman, Sen. Jerry Moran, R-Kan., put it, cyber insurance "may be a market-led approach to help businesses improve their cyber security posture by tying policy eligibility or lower premiums to better cyber security practices."

Meanwhile, several bills have been introduced in Congress — the most recent one last week — to promote more information sharing between public and private entities concerning cyber breaches.

Congressional interest in cyber insurance is a "natural extension" of lawmakers' examination of cyber security issues, said Michael Menapace, counsel in the Hartford, Connecticut, office of Wiggin and Dana L.L.P. and an adjunct professor of law at Hamden, Connecticut-based Quinnipiac University.

Mr. Menapace, who testified before Sen. Moran's panel, said after the hearing the congressional concern over how the costs of cyber breaches will be covered is "naturally going to lead you to insurance. Insurers certainly have influence over their practices that are employed by the insureds."

He added that insurers themselves hold a lot of data, so their own experience in this area is valuable.

Another witness — Ben Beeson, the Washington-based vice president for cyber security and privacy with Lockton Cos. L.L.C. — agreed, saying cyber insurance is an important market force that can drive improved cyber security for companies.

Speaking before the panel, Mr. Beeson said Lockton and "we believe the industry as a whole" would welcome the introduction of legislation that would reduce barriers and encourage organizations to share cyber threat indicators with the government and each other while also protecting individual privacy.

In an interview after the hearing, Mr. Beeson called the hearing "hugely important for our clients and industry."

"How do you get industry (companies) to raise its game, to improve its resilience against that type of threat?" he said. "I don't think you can legislate minimum security standards. It's about an approach, a culture. It's very difficult to be prescriptive."

Congress would rather see the market try to help solve the problem, Mr. Beeson said. "It puts the insurance industry in a place perhaps where it didn't expect to be: Congress says, 'We want you at the front of the conversation.' "

Cyber insurance can help address two fundamental cyber security problems, Mr. Beeson said: industry not investing enough in security; and the other of determining the right approach to security, which, he said, is tackling it in an enterprise risk management framework.

"It's a huge opportunity; we're asking the government to do anything they can do to provide more incidence data," Mr. Beeson said.

During his testimony, Mr. Menapace said there's no single standard for private and public entities requiring reporting of data breaches. Instead, each state has its own standard, leading to increased costs and inefficiency, he said.

Mr. Beeson said Congress could follow a precedent in health care reporting and set a federal notification requirement, a good move for consumers and businesses.

Representatives of insurer groups agreed.

"It would be nice to have a single federal standard" for companies regarding data security breach reporting, said Alex Hageli, a director at the Chicago-based Property Casualty Insurers Association of America. "It's been on the wish list for some time, and it seems with all of the recent breaches that it might actually come to fruition."

"Ideas, which all the panelists endorsed, such as federal legislation encouraging sharing of cyber threat data, exploring the creation of a data repository and a pre-emptive federal data breach standard, should help improve underwriting and increase market capacity," a spokesman for the Washington-based American Insurance Association said. "We feel that greater collection of information about the market would be a good thing."

PCI's Mr. Hageli also said that the Federal Insurance Office has been "very interested in developing the cyber insurance market."

"We feel cyber insurance is a key piece of the puzzle of how to best prepare our country to address cyber threats. It was great to see the Senate hold what was the first-ever hearing on this issue," said Jonathan Bergner, federal affairs director in the Washington office of the National Association of Mutual Insurance Cos.

Laura Foggan, a partner in the Washington law firm Wiley Rein L.L.P. who specializes in insurance law, said she thinks there is "pretty broad" insurance industry support for legislation that encourages information sharing about cyber security breaches.

FEW U.K. FIRMS BOTHER WITH CYBER COVER

Sarah Veysey
30 March 2015
Business Insurance

U.K. buyers often have very different concerns than U.S. buyers when it comes to transferring cyber risks to insurance, an issue that insurers, brokers, buyers and the U.K. government are looking to rectify.

The rapidly growing risk is an issue for U.K companies and organizations, according to a report issued last week by the U.K. government, Marsh L.L.C. and insurers. While 81% of large U.K. companies and 60% of small ones suffered a cyber security breach in the past year, less than 10% have bought cyber insurance.

A lack of data pooling has hampered insurers' ability to develop coverage and pricing models. In addition, the potential of aggregated losses affecting a large number of companies is a concern for insurers, according to the analysis.

"This is a call to arms to the insurance sector," said Mark Weil, London-based CEO of Marsh in the United Kingdom and Ireland, as many large companies still do not view cyber coverage as "part of the toolkit" to manage cyber risks.

The joint initiative of the U.K. Cabinet Office, Marsh and 13 insurers that produced the cyber report is "a first step" to help businesses manage their cyber risks, said Natalie Black, London-based deputy director of cyber defense and incident management at the Cabinet Office.

The report recommends establishing a forum including the government and the insurance sector, such as the Association of British Insurers and Lloyd's of London, on "data and insight exchange for policy discussions," among other things.

"The London market has a long, proud history of finding innovative solutions to insuring large, complex risks that are challenging to underwrite locally," Lloyd's CEO Inga Beale said. "Just as the market has responded to new challenges before, so it needs to again."

John Hurrell, CEO of London-based Airmic Ltd., said cyber coverage developed so far largely responds to a data breach, which is a huge concern for U.S. buyers. However, some U.K. buyers are more worried about theft of intellectual property, disruption of services and reputational damage, he said. Also, there often is insufficient capacity to provide limits large buyers desire, the leader of the U.K. risk management group said.

Sharing information among firms and insurers on cyber incidents could help the U.K. cyber insurance market, said Sarah Stephens, a London partner in the financial lines group at JLT Speciality Ltd., a Jardine Lloyd Thompson Group P.L.C. unit.

TREND; UK GOVERNMENT AND INSURANCE MARKET IN JOINT INITIATIVE ON CYBER RISK

25 March 2015
Insurance Newslink

With 81% of large UK businesses and 60% of small companies suffering a cyber security breach in the last year, a report published on Monday by HM Government and Marsh announced a new set of joint initiatives between Government and the insurance sector to help firms get to grips with cyber risk; to establish cyber insurance as part of firms' cyber tool-kits and cement London as the global centre for cyber risk management.

The report, entitled "UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk", has been produced in collaboration with the UK's insurance market and a number of top UK companies, and aims to make the UK a world centre for cyber security insurance. In particular, it highlights the exposure of firms to cyber attacks among their suppliers with a key agreement that participating insurers will include the Government's Cyber Essentials certification as part of their risk assessment for small and medium businesses.

Mark Weil, ceo of Marsh UK & Ireland, comments "While critical infrastructure in regulated sectors, such as banks and utility firms, are used to this kind of risk, most firms are not and their risk management practices are geared around lower-level, slower moving risks. Companies will need to upgrade their risk management substantially to cope with the growing threat of cyber attack, including introducing disciplines such as stress-

testing, and creating a joined-up recovery plan that brings together financial, operational, and reputational responses."

Francis Maude, Minister for the Cabinet Office and Paymaster General said "It is part of this Government's long-term economic plan to make the UK one of the safest places in the world to do business online. The UK's insurance market is world renowned and we want it to be the same in relation to cyber risks. The market has extensive knowledge and experience of more established risks to help businesses manage and mitigate relatively new cyber risks.

Insurance is not a substitute for good cyber security but is an important addition to a company's overall risk management. Insurers can help guide and incentivise significant improvements in cyber security practice across industry by asking the right questions of their customers on how they handle cyber threats."

Key findings from the report are:

-Insurers can help firms better manage their cyber risks. By asking the right questions and educating clients, insurers can help drive the adoption of cyber security best practice, including Cyber Essentials.

-The UK insurance sector is already a world-leader. With initiatives like this, the sector is demonstrating that the UK is the natural home for a growing global cyber insurance market.

-Insurers support shows the success of Government's Cyber Essential Scheme. They recognise having Cyber Essentials certification is a valuable indicator of a mature approach to cyber security in SMEs that contributes to the reduction of risk

-The contributing insurers will incorporate Cyber Essentials into their risk assessment process for SMEs, making it easier for firms to get coverage.

-Firms place cyber amongst their leading risks in terms of likelihood and severity of impact

-Banks and national infrastructure organisations are generally better equipped in modelling cyber risks which can be very fast moving and damaging whereas most other businesses are not as well equipped to deal with this type of 'tail risk'

-Modelling of cyber risk has been difficult due to a lack of available data. However, there are alternative approaches to valuing the risk of cyber attack including using stress testing.

-There is a lack of awareness of cyber insurance and certainty about coverage–less than 10% of companies have cyber insurance according to recent surveys

-A lack of data pooling poses a challenge for the insurers in the development of their pricing models and coverage

-The potential for the aggregation of losses impacting a large number of firms and arising from a single attack, leading to losses across a large number of firms, is a growing concern for insurers

-The UK insurance market has a history of underwriting large complex risks and has established itself to be a leading market in the provision of cyber insurance.

Recommendations include:

For insurers and Government

-Participating insurers will include the Cyber Essentials certification as part of their cyber risk assessment for SMEs when backed by a suitable insurance policy in order to improve their supply chain resilience. This will simplify the application process for businesses.

-A new forum will be established by HM Government with the insurance sector, including the ABI and Lloyd's, on data and insight exchange for policy discussions.

For businesses

-Firms should review their management of cyber risk. Effective risk management needs to include a Board-level owner for cyber risk, a joined up recovery plan and the use of stress testing to confirm financial resilience against cyber threats

For insurance brokers

-Participating insurers will include Cyber Essentials accreditation as part of their risk assessment for SME to encourage greater adoption. Marsh will launch a new cyber insurance product for SMEs which will absorb the cost of Cyber Essentials certification for the majority of firms. HMG encourages other brokers to follow suit.

-Brokers should provide firms with a cyber assurance statement to give the Board confidence of the completeness of their cover.

For the market

-Lloyd's will work with UKTI to market the cyber capabilities of the London Market globally

-A new multi-disciplinary taskforce set up by CityUK aimed at bringing together different sectors to accelerate discussions on a joint UK cyber offering related to insurance for export.

This article is supplied by Only Strategic Financial Newslink (www.onlystrategic.com)

DIVERSE RECRUITMENT REQUIRED IF LONDON IS TO SECURE GLOBAL CYBER DOMINANCE

Francesca Nyman
24 March 2015
Post Magazine

Greater cross-industry collaboration and a significant recruitment drive are needed if London is to fulfil its ambition to become a global cyber insurance hub, according to London market firms.

Earlier this week (24 March), in a report published in conjunction with global broker Marsh, the government unveiled its target for London to become a cyber hub capable of supporting the country's cyber-exposed corporates and exporting its expertise on the global stage.

The UK government's annual breach report shows that 81% of large businesses and 60% of small businesses suffered a security breach in 2014.

Several attempts have been made to quantify the economic cost of cyber crime on UK businesses and, while there are a wide range of estimates, figures consistently range in the billions of pounds.

Although significant cyber experience already sits within the London market, this alone will not ensure the capital retains a position of dominance, according to cyber underwriters.

Matthew Webb, head of technology, cyber and data at Hiscox UK, told Post transforming London into a hub of cyber insurance was "a realistic ambition" but stressed that it required "a joined-up approach".

"While the figures released in this report indicate the size of potential exposure, the reality is that many [cyber] incidents currently go unreported or - even worse - undiscovered. Companies struggle to understand cyber risk and many brokers admit to not having the confidence to speak to their clients about it, so there's much to be done," he explained.

"The key will be having the right people and the right products to address customer needs, both now and in the future. If we are to steal a march on other geographies, who may also have their sights set on becoming a cyber insurance hub, then it's crucial we act now," he added.

Meanwhile, Jason Harris, CEO for international property and casualty insurance at XL Group, said that to claim the top spot for cyber underwriting, London must "develop more talent from diverse backgrounds and continually invest in staying current in this incredibly fast changing landscape".

"Outside of the cyber class, as an industry we also need to raise our knowledge game. The reality is that the exposure from technology or ‘cyber' cuts across classes and needs to be viewed as such. If you look at what drives a business, it's technology, across all levels," he added.

Paul Bantick, head of Beazley's UK and international TMB team, said that from an insurance standpoint London was "already a cyber hub" in the area of US data breach cover but said that to attract business from jurisdictions outside the US and UK it needed to develop more local language expertise.

"While there is significant data breach expertise sitting in London and there's a lot of business that is currently written and insured here, if we're going to do that and we're going to drive that throughout Europe then we need to have people who can do that in the local language. We need products that can respond in the local language," he said.

Chris Croft, head of the secretariat of the London Market Group, whose London Matters report in November last year highlighted a trend of risks that had previously come to London increasingly remaining in local markets, said the collaboration between government and industry was "encouraging".

"A key suggestion from the report was that London had lost its ability to innovate and cyber is an area that needs a lot of innovation so anything that is being done to attract that to the market should be welcomed," he said.

LMA CEO David Gittings added that the report "should help raise awareness of businesses both to the increasing risk and the availability of specific cyber insurance to protect assets and revenue streams".

However, he said it also outlined a number of hurdles that the industry would need to overcome.

"The report highlights concern around the paucity of data and the challenges facing insurers around risk pricing and essentially, modelling and mitigation of risk aggregation," he told Post.

One issue that has polarised opinion is the potential establishment of a facility similar to the Pool Re terrorism scheme for cyber aggregation risk.

Government and industry have opted not to create such a facility, although Marsh UK and Ireland CEO Mark Weil said the matter was "hotly debated" during the course of the pre-report consultation.

While he stopped short of calling for a government back-stop, Shaun Crawford, global head of insurance at EY, said the burden "should not lie solely at the feet of insurers, and the security industry as a whole should be involved".

"Cyber risk is different to any other type of insurable risk because it is much more dynamic in nature, so whilst insurers have the experience of managing risk, the traditional approach and methodology cannot be applied."

Tom Hoad, enterprise risk underwriter at Tokio Marine Kiln, told Post that in time "there may well be a place for a government-backed [facility] to provide some kind of risk transfer".

2% OF UK FIRMS INSURED AGAINST CYBER ATTACKS

24 March 2015
PANAPRESS - Pan African News Agency

Just 2% of large UK firms have specialised insurance cover against cyber attacks, according to a report published today. This figure dropped close to zero for smaller companies and around half of the CEOs interviewed were unaware that cyber risks can be insured.

Furthermore, business leaders who were aware of cyber insurance solutions "tend to overestimate" the extent to which they are covered, with surveys showing 52% of CEOs believed that they had cover when less than 10% actually did.

The report was jointly published by the government and Marsh, a global leader in insurance broking and risk management, and is the result of the government working closely with the insurance sector following a summit regarding cyber attacks in November 2014.

New joint initiatives between the government and the insurance sector were also announced to help firms address the problem and cement London as the global centre for cyber risk management.

Mark Weil, CEO of Marsh UK & Ireland, said companies must upgrade their risk management substantially to cope with the growing threat of cyber attacks.

Last year 81% of large UK businesses and 60% of small companies suffered a cyber security breach, costing the UK economy billions of pounds, almost double what it was in 2013.

Almost 90% of FTSE 350 companies now include cyber risk within their strategic risk report, up from 58% in 2013.

The London cyber insurance market makes up around 10% of the global market, netting £160 million in premiums, yet the report revealed that policies for UK companies currently only account for an estimated £20-25 million - 1.5% of the global market.

According to the report, while larger firms have taken some action to make themselves more cyber-secure, they face an escalating threat as they become more reliant on online distribution channels and as attackers grow more sophisticated.

Weil said: "While critical infrastructure in regulated sectors, such as banks and utility firms, are used to this kind of risk, most firms are not and their risk management practices are geared around lower-level, slower moving risks."

He urges firms to create a joined-up recovery plan that brings together financial, operational and reputational responses and introduce disciplines such as stress-testing.

Francis Maude, minister for the Cabinet Office and paymaster general, said this recommendation is part of this government's long-term economic plan to make the UK one of the safest places in the world to do business online.

"The UK's insurance market is world renowned and we want it to be the same in relation to cyber risks. The market has extensive knowledge and experience of more established risks to help businesses manage and mitigate relatively new cyber risks," he said.

He added insurance is not a substitute for good cyber security but an important addition to a company's overall risk management.

"Insurers can help guide and incentivise significant improvements in cyber security practice across industry by asking the right questions of their customers on how they handle cyber threats," he said.

UK AIMS TO BECOME WORLD CENTRE IN CYBER SECURITY INSURANCE

24 March 2015
Jpost.com (The Jerusalem Post online edition)

The UK aims to become a global leader in cyber security insurance through a newly announced set of joint initiatives between the government and the insurance sector.

The initiatives are designed to help firms get to grips with cyber risk, to establish cyber risk insurance as part of firm's cyber tool kits and to establish London as the global centre for cyber risk management.

The plan is detailed in a report published by the government and Marsh, one of the UK's leading insurance brokers and risk advisors.

The report follows a meeting in November 2014 between Cabinet Office minister Francis Maude and 13 major insurance firms to discuss ways of improving how UK businesses manage cyber security risk.

The report builds on the 10 Steps to Cyber Security guidance on managing cyber risk and the Cyber Essentials Scheme to ensure basic cyber hygiene as part of the UK Cyber Security Strategy.

Those at the meeting agreed to work together to develop proposals to improve the availability and uptake of cyber insurance by UK companies.

A joint working group was set up and has produced a definitive report on the UK cyber insurance market, providing key statistics, findings, insights and key recommendations.

According to the report, 81% of large UK businesses and 60% of small companies suffered a cyber security breach in the past year.

The report, entitled UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk, highlights the exposure of firms to cyber attacks among their suppliers.

A key agreement detailed by the report is that participating insurers will include the government's Cyber Essentials certification as part of their risk assessment for small and medium-sized enterprises (SMEs).

A key initiative announced in the report is that Marsh is to launch a new cyber insurance product for SMEs which will absorb the cost of Cyber Essentials certification for the majority of firms.

The government has encouraged other brokers to follow suit. The cost of certification has been identified by a number of commentators as being the biggest obstacle to SMEs.

Cyber threats are estimated to cost the UK economy billions of pounds each year with the cost of cyber attacks nearly doubling between 2013 and 2014.

The report revealed hat, while larger firms have taken some action to make themselves more cyber secure, they face an escalating threat as they become more reliant on online distribution channels and as attackers grow more sophisticated.

The report issues a call to arms for insurers and insurance brokers to simplify and raise awareness of their cyber insurance offering, and to ensure that firms understand the extent of their coverage against cyber attack.

Companies are recommended to stop viewing cyber largely as an IT issue and focus on it as a key commercial risk affecting all parts of its operations. The report also recommends that firms examine the different forms of cyber attacks they face, to stress-test themselves against them and to put in place business-wide recovery plans.

The report also notes a significant gap in awareness around the use of insurance, with around half of firms interviewed being unaware that insurance was available for cyber risk.

Other surveys show that despite the growing concern among UK companies about the threat of cyber attacks, fewer than 10% of UK companies have cyber insurance protection even though 52% of chief executives believe their companies have some form of coverage in place.

The UK government is hosting an event at the Cabinet Office on 23 March 2015 for senior executives of insurers and top UK companies on the role of insurance in managing growing cyber threats.

Maude, who has overseen the UK cyber security strategy, said in a statement that it is part of the government's long-term economic plan to make the UK one of the safest places in the world to do business online.

"The UK's insurance market is world-renowned and we want it to be the same in relation to cyber risks. The market has extensive knowledge and experience of more established risks to help businesses manage and mitigate relatively new cyber risks," he said.

However, Maude said insurance is not a substitute for good cyber security, but is an important addition to a company's overall risk management.

"Insurers can help guide and incentivise significant improvements in cyber security practice across industry by asking the right questions of their customers on how they handle cyber threats," he said.

Marsh UK & Ireland chief executive Mark Weil said that while critical infrastructure in regulated sectors, such as banks and utility firms, are used to this kind of risk, most firms are not and their risk management practices are geared around lower-level, slower-moving risks.

"Companies will need to upgrade their risk management substantially to cope with the growing threat of cyber attack, including introducing disciplines such as stress-testing, and creating a joined-up recovery plan that brings together financial, operational and reputational responses," he said.

Key findings of the report:

Insurers can help firms better manage their cyber risks. By asking the right questions and educating clients, insurers can help drive the adoption of cyber security best practice, including Cyber Essentials.

The UK insurance sector is already a world-leader. With initiatives like this the sector is demonstrating that the UK is the natural home for a growing global cyber insurance market.

Insurers support shows the success of government's Cyber Essential Scheme. They recognise having Cyber Essentials certification is a valuable indicator of a mature approach to cyber security in SMEs that contributes to the reduction of risk.

The contributing insurers will incorporate Cyber Essentials into their risk assessment process for SMEs, making it easier for firms to get coverage.

Firms place cyber amongst their leading risks in terms of likelihood and severity of impact.

Banks and national infrastructure organisations are generally better equipped in modelling cyber risks which can be very fast moving and damaging whereas most other businesses are not as well equipped to deal with this type of "tail risk".

Modelling of cyber risk has been difficult due to a lack of available data. However, there are alternative approaches to valuing the risk of cyber attack including using stress testing.

There is a lack of awareness of cyber insurance and certainty about coverage - fewer than 10% of companies have cyber insurance according to recent surveys.

A lack of data pooling poses a challenge for the insurers in the development of their pricing models and coverage.

The potential for the aggregation of losses impacting a large number of firms and arising from a is a growing concern for insurers.

The UK insurance market has a history of underwriting large complex risks and has established itself to be a leading market in the provision of cyber insurance.

Key initiatives and recommendations of the report:

Participating insurers will include the Cyber Essentials certification as part of their cyber risk assessment for SMEs when backed by a suitable insurance policy in order to improve their supply chain resilience. This will simplify the application process for businesses.

A new forum will be established HM Government with the insurance sector, including the Association of Business Insurers and Lloyds, on data and insight exchange for policy discussions.

Firms should review their management of cyber risk. Effective risk management needs to include a board-level owner for cyber risk, a joined up recovery plan and the use of stress testing to confirm financial resilience against cyber threats.

Participating insurers will include Cyber Essentials accreditation as part of their risk assessment for SME to encourage greater adoption.

Brokers should provide firms with a cyber assurance statement to give the Board confidence of the completeness of their cover.

Lloyds will work with UK Trade & Investment to market the cyber capabilities of the London Insurance market globally.

A new multi-disciplinary taskforce set up by CityUK is aimed at bringing together different sectors to accelerate discussions on a joint UK cyber offering related to insurance for export.

ACE LAUNCHES DEDICATED CYBER RISK UNIT

15 March 2015
Asia Insurance Review

ACE Group launched a new, independent cyber risk business unit early this year as it continues to strengthen its local underwriting and risk management capabilities across Continental Europe and build its market leadership in this growing area of emerging risk.

Following research by ACE which indicates that cyber is a “top three” emerging issue for European risk managers, the launch represents a further evolution of the work of ACE’s global cyber practice, first established in 2014.

ADDITIONAL MATERIAL

WEBSITES

The following websites contain information on the number, source and incidences of cyber attacks, data breaches etc. Some of them also include names of the companies involved. This is information that can be shared externally as it is from public domain sources.

ADVISEN FPN: CYBER EDITION

http://cyberfpn.advisen.com/#top

Free newsletter of cyber news published by Advisen.

BOOZ ALLEN CYBER TAB

https://cybertab.boozallen.com/

CyberTab is an anonymous, free tool that helps information-security and other senior executives understand the damage to companies inflicted by cyber crime and attacks

BREACH LEVEL INDEX – SAFE NET

http://www.breachlevelindex.com/index.html#sthash.gODzFNWn.dpbs

Live site showing number of data breaches and statistics for industries and source. There is also a list of recent incidents and a risk calculator.

DEUTSCHE TELECOM'S CYBER INITIATIVE

http://www.sicherheitstacho.eu/info

Overview of current cyber attacks; top 15 source countries (last month); distribution of attack targets (last month) and overall sum of attackers per day (last month).

DIGITAL ATTACK MAP - ARBOR

http://www.digitalattackmap.com/

Top daily DDoS attacks worldwide. Needs to be viewed in Chrome or IE9.

HACKMAGEDDON.COM

http://hackmageddon.com

Specialist blog that tracks cyber attacks and incidences. A time line is published regularly. Material can be shared externally in presentations etc provided it is credited to the Hackmageddon.com blog.

REPORTS

Reports can be downloaded from an FTP site: ftp://adbftpdevl.chartisinsurance.net/London/Cybercrime%20-%20Reports%20-%20NVAR/. Material is available for approximately 6 weeks. Please save any reports you want to keep locally. Many of these reports are from public domain sources and can be shared externally.

THE TRUE COST OF DATA BREACHES IN THE PAYMENTS INDUSTRY – SMART CARD ALLIANCE MAR15

Data breaches are increasingly impacting businesses across the globe, with the average cost paid by a breached organization reaching $5.9 million at the end of 2014.

UK CYBER SECURITY - MARSH 2015