

AUGUST 2011

INFORMATION UPDATE:

The following information reflects the lists handled for August 2011:

TRACKER

Lists: 15
Records: 443
Hits: 140

SAPS 13

Lists: 50
Records: 887
Hits: 207

ENQUIRIES

Enquiries: 74
Replies: 272

INSIDE THIS ISSUE...

| | |
|-----------------------------|----------|
| SAICB UPDATE | 1 |
| FRAUDLINE | 1 |
| ARTICLE—SERVAMUS | 2 |
| ARTICLE—ARRIVE ALIVE | 4 |
| ARTICLE—BANKTECH | 5 |
| CONTACT | 9 |

SAICB UPDATE

SAICB UPDATE

August 2011 has been a month of review and reconciliation of the past year's successes and the consolidation of cases in the year ahead in terms of the status of the cases, allocation of resources and expected outcome dates for the projects / cases under investigation.

To date the SAICB and its members have successfully prosecuted with convictions and sentencing in 6 cases through our courts. The SAICB has 10 current projects under full investigation for completion over the next two years, and 10 new cases under investigation but not yet registered as projects. This is a huge case load for our organization, but with our investigators, member company representatives and support staff, all working efficiently and effectively together, it is being managed very successfully.

The participation of the South African Police (SAP), National Prosecuting Authority (NPA), NPA Assets Forfeiture and SARS in our cases from the registration of our projects has ensured the successful prosecutions of our cases to date, and these partnerships and relationships have been one we are particularly proud of.

While identifying the syndicates is a very important aspect of what the SAICB does, establishing and understanding the Modus Operandi (MO) of the syndicates is also important. This allows us to track other syndicates using the same or similar MO to defraud the industry, in our data.

UPDATE:

To recap the MO and case mentioned in the July 2011 edition:

The suspect used unsuspecting valid peoples ID numbers and opened insurance policies in their names with the same bank accounts and PO Box numbers. After investigation it was found that the risk addresses that were used did not exist. He phoned the insurance company and lodged a claim and when the assessor tried to contact him to assess the claim they would not be able to get a hold of him. He would phone after a month and berate them for the slow service, the claim was then settled expeditiously.

The suspect was arrested and the following seized: 39 cell phones; 50 sim cards; 4 laptops; ID documents for 69 persons identified in the investigation; letters to different banks giving the target permission to use the bank accounts; 150 Policy documents to date; invoices and

FRAUDLINE

In July 2011, 20 reports were received of which 14 reports were for the short term insurance industry, 1 report was received for brokers and 5 reports for the Life industry.

Since 2002, 27161 reports have been received of which 917 reports were for the short term industry 137 reports for the brokers and 371 reports were for the life industry.

For further information on the statistics, please contact

Melanie Pillay on melaniep@saicb.co.za



0860 002526
insurance@fraudline.co.za

MEMBERS

SANTAM
 MUTUAL & FEDERAL
 HOLLARD
 LION OF AFRICA
 REGENT
 TELESURE
 ABSA INSURANCE
 STANDARD BANK
 INSURANCE
 OUTSURANCE
 MOMENTUM
 MIWAY
 ALEXANDER
 FORBES

PARTNERS

SOUTH AFRICAN
 INSURANCE
 ASSOCIATION (SAIA)
 TRANSUNION
 FRAUDLINE
 MEMEX
 SAFPS
 UNICODE
 BACSA
 NEWORDER
 DATADOT
 CGC
 SAVRALA

ARTICLE— SAICB FEEDBACK CONT...

quotes.

The suspect applied for bail, and was released on R10 000 bail, with the provision that he report to a police station twice a week. Current value of the case is R1 million, and he is to appear in court again on 28 September 2011. Another 11 cell phones were seized, which were linked back to false claims as per the cell phone fraud mentioned in the MO last month. It was also found that he used the false IDs mentioned to get loans at banks and did not repay them, and the accounts holders could not be traced because the details used were false.

Latest arrest: Suspect bought a salvage vehicle, staged an accident and claimed from one of our member companies - Value – R400 000. The suspect was arrested and is in the process of plea bargaining with the state.

In the coming month it is anticipated that another 12 arrests in two cases will be made, details of these cases and arrests will appear in the next issue.

August 2011 edition...

This months issue pays particular attention to the UN's "Decade of Action for Road Safety" launched earlier this year and South Africa's commitment to addressing the over 14000 annual deaths experienced on South African roads as part of our countries strategy for road safety.

The SAICB has been at the forefront of making the industry aware of the issues regarding cyber security in the financial industry and this issue has a very informative article on the threats to the banking community and the how to manage the risk.

FOR MORE INFORMATION ON ANY OF OUR INITIATIVES, PLEASE FEEL FREE TO CONTACT MELANIE PILLAY ON melaniep@saicb.co.za

ARTICLE—SERVAMUS

ROAD SAFETY - A DECADE OF ACTION

The number one killer of people around the world is not a virus. It is a man-made hazard: vehicle crashes.

More than 14 000 people die annually on South African roads due to vehicle accidents, but the worldwide incidence of road accidents claim the lives of approximately 1.3 million people annually - equating to more than 3000 deaths each day. More than a half of these people did not travel in a vehicle, while 90% of these accidents occur in developing countries. Adding this information to the prediction that vehicle ownership across the world will double by 2020, it becomes clear that the situation spells disaster!

The question is: what are we going to do about this shocking reality? The United Nations called for a Decade of Action for Road Safety that is intended to run from 2011 to 2020. On 11 May 2011 more than 100 countries around the world launched this global plan, which is based

ARTICLE— SERVAMUS CONT...

on five pillars:

Pillar 1 - Road safety management. This pillar focuses on the need to strengthen institutional capacity to further national road safety efforts. It includes activities such as establishing a lead agency for road safety in each country involving partners from a range of sectors; developing a national road safety strategy; and setting realistic and long term targets for activities with sufficient funding for their implementation. It also calls for the development of data systems to monitor and evaluate activities.

Pillar 2 - Safer roads and mobility. This pillar highlights the need to improve the safety of road networks for the benefit of all road users, especially the most vulnerable: pedestrians, cyclists and motorcyclists. Activities include making the planning, design, construction and operation of roads more safety conscious, and ensuring that roads are regularly assessed for safety; encouraging the relevant authorities to consider all forms of transport and types of safe infrastructure when they respond to the mobility needs of road users; and promoting road safety training and education on these topics.

Pillar 3 - Safer vehicles. This pillar addresses the need for improved vehicle safety by encouraging the harmonisation of relevant global standards and mechanisms to accelerate the uptake of new technologies which impact on safety. It includes activities such as implementing new vehicle assessment programmes so that consumers are aware of the safety performance of vehicles, as well as trying to ensure that all new motor vehicles are equipped with the minimum level of safety features, such as seatbelts. Other activities covered include promoting more widespread use of crash avoidance technologies which have proven effectiveness, such as electronic stability control and anti-lock braking systems.

Pillar 4 - Safer road users. This pillar focuses on developing comprehensive programmes to improve road user behaviour. Activities include the sustained or increased enforcement of road safety laws and standards, combined with public awareness and education to increase the wearing of seatbelts and helmets and to reduce drinking and driving, speeding and other risky behaviour. It also calls for activities to reduce work related road traffic injuries and promotes the establishment of graduated driver licensing programmes for novice drivers.

Pillar 5 - Post crash response. This pillar promotes the improvement of the medical industries and other systems to provide appropriate emergency treatment and longer term rehabilitation for crash victims. Activities include developing pre hospital care systems, including the implementation of a single nationwide telephone number for emergencies; providing early rehabilitation and support to injured patients and those bereaved by road traffic crashes; establishing insurance schemes to fund such initiatives; and encouraging a thorough investigation into crashes coupled with an appropriate legal response.

During the next few months SERVAMUS will discuss some of these pillars in more depth.

On 7 and 8 June 2011 the South African Road Safety Federation (SARF) and the Road Traffic Management Corporation (RTMC) hosted an International Road Safety Conference in Pretoria. This conference followed the launch of the Decade of Action for Road Safety and was aimed at establishing strategies to reduce road deaths by 2020. National and international experts in the field of road safety addressed the delegates during the two day conference.

During his address, the Deputy Minister of Transport Mr Jeremy Cronin said that road crashes are the number one cause of unnatural child deaths in South Africa. Therefore, he said, it is a huge children's rights issue. However, it is not only a human rights struggle (a struggle to uphold the right to safety) but also an economic struggle, as road crashes cost South Africa millions of Rands annually. "We have a crisis on hands," he said, "We must work together and that also means that we must learn from other countries."

ARTICLE—SERVAMUS CONT...

We all know someone who has been involved in a road accident, so why don't we start changing our behaviour on the road? We could start by sticking to the basics such as reducing speed, buckling up, avoiding talking on our cell phones while driving, and not drinking and driving. Remember: road safety starts with me and you!

THANK YOU TO KOTIE GELDENHUYS FOR PERMISSION TO USE THIS ARTICLE THAT APPEARED IN THE AUGUST 2011 EDITION OF SERVAMUS. FOR FURTHER INFORMATION PLEASE CONTACT KOTIE ON kotie@servamus.co.za

ARTICLE—ARRIVE ALIVE

Department Of Transport

Transport Minister confirms need for changes in approach to road safety
23 August 2011

Transport Minister Sibusiso Ndebele has said that South Africa can no longer afford a business-as-usual approach to road safety. Addressing Transport MECs and senior officials at a MinMec meeting in Cape Town earlier today (23 August), Minister Ndebele called on MECs to ensure that road safety programmes in the various provinces are intensified in line with the United Nations Decade of Action for Road Safety 2011-2020.

"South Africa can no longer afford a business-as-usual approach to road safety. The month of August has been horrific in terms of road crashes and deaths, particularly in KwaZulu-Natal. Provinces and municipalities should already be putting in place road safety plans for September to ensure there is no recurrence of what happened on our roads during August.

"Each province and municipality must know where, when, why, who, what and how in terms of road deaths in their respective areas. MEC's and Mayors must ensure that all Traffic Chiefs provide a detailed weekly evaluation and analysis of road deaths for their policing areas, as well as corrective measures being implemented. There must be active participation from national, provincial and local government in this **Decade of Action for Road Safety**. We will be entering into Service Level Agreements with provinces and municipalities with specific road safety targets.

"These tragic deaths and the misery and grief they cause are not inevitable. They can be prevented, if measures are taken by all of us to ensure safe roads. We are therefore calling upon all South Africans to play your part in this Decade of Action," said Minister Ndebele.

The meeting agreed that the following five priorities must be urgently addressed by provinces and municipalities:

- Improvement in the methodology and collection of road traffic crash data;
- Service Level Agreements to be concluded with regards to transport deliverables, particularly road safety and traffic law enforcement;
- Licensing Centres – The Road Traffic Management Corporation (RTMC) to intensify investigations into acts of corruption and poor service delivery and provide recommendations.
- Enforcement on drunk driving to be stepped up.
- Provision of 24-hour traffic law enforcement to be rolled out across the country.

Other issues discussed at the meeting included the RTMC turn-around strategy, launch of the SADC Decade of Action for Road Safety, status report of the R22-bn S'hamba Sonke Road Maintenance Programme targeting the repair of potholes

ARTICLE—ARRIVE ALIVE CONT...

and maintenance of the secondary road network, October Transport Month as well as report back from the mid-year Cabinet Lekgotla.

MinMec is a coordinating body chaired by the Minister and primarily comprises of the Deputy Minister, nine MECs for Transport and other key officials.

THANK YOU TO JOHAN JONCK FOR PERMISSION TO USE THIS ARTICLE THAT APPEARED ON THE ARRIVE ALIVE WEBSITE. FOR FURTHER INFORMATION PLEASE CONTACT JOHAN ON jonckie@arrivealive.co.za OR GO TO WEBSITE: www.arrivealive.co.za . FOR THE FULL GLOBAL PLAN ON THE UN DECADE OF ROAD SAFETY PLEASE GO TO: http://www.arrivealive.co.za/Decade_Road_Safety/Decade%20of%20Action%20for%20Road%20Safety

ARTICLE—BANKTECH

COULD A MAJOR SECURITY BREACH BE ON THE HORIZON?

By Lisa Valentine

Love him or hate him, Julian Assange, the infamous director of WikiLeaks, has heightened awareness of the dangers of sensitive information leaking out of an organization. Although financial institutions have to date largely escaped the fate of the U.S. government and other industries, security experts warn that it's only a matter of time until a bank suffers a major breach from a cyber attack.

Indeed, the largest industry targeted by criminals is financial services, according to the "[2010 Data Breach Investigations Report](#)" from Verizon Business (New York) and the United States Secret Service (USSS). Not only did financial services represent 33% of the more than 900 breaches studied over a six-year span, the industry also accounted for a staggering 94% of all compromised records.

Today's cyber attacks are more targeted -- and more dangerous -- than in the past. "Attacks are 'low and slow' in that criminals are pinpointing specific institutions and patiently and painstakingly infiltrating the organization to remove precise data," explains Jonathan Penn, vice president, Forrester Research (Cambridge, Mass.).

Advanced Persistent Threats (APTs) illustrate the persistence of today's cyber criminals. RSA (Bedford, Mass.), which supplies security solutions to some of the world's largest financial services firms, announced in March that data related to its SecurID authentication tokens was stolen via an APT attack. APT has become a euphemism for attacks carried out by sophisticated, well-funded hackers--often linked to the Chinese government--that are executed methodically over long periods of time.

Not only do banks need to protect themselves from criminals outside the organization, they also need to protect against internal information leakage from employees, contractors, partners and vendors. "Someone intentionally taking and sharing information is an incredibly difficult problem to solve," notes Richard Mackey, vice president of consulting, SystemExperts Corp. (Sudbury, Mass.).

The recent media reports of leaked emails from a former Bank of America employee to the online hacker group Anonymous turned into a case of "much ado about nothing," but highlight how easily an information leak can occur.

The internal threat is real: According to Verizon, internal agents caused nearly half (48%) of financial services breaches. However, financial institutions are largely unprepared.

ARTICLE—BANKTECH CONT...

Although 56% of senior security executives are very confident about thwarting external breaches, only 34% display the same confidence about internal threats, according to Deloitte's "2010 Financial Services Global Security Survey."

The Smartphone Dilemma

The pervasiveness of mobile devices complicates security for banks. Employees are clamouring to use their mobile devices of choice at work, but security managers are still struggling to secure new, increasingly powerful devices.

Smartphones in particular are exploding in popularity, presenting the proverbial "good news/bad news" scenario for financial institutions. George Peabody, director of Emerging Technologies Advisory Service at consultancy Mercator Advisory Group (Maynard, Mass.), predicts that 60% of mobile phone subscribers will have smartphones by 2012. Since the criminals "move to where the people are," expect malware to proliferate on iPhones, Androids and other mobile devices, says Peabody.

A.N. Ananth, CEO of security solutions provider Prism Microsystems (Columbia, Md.), describes three approaches banks can take to manage mobile device security. The first approach is to lock down the environment. Doing so, however, can make the carrier less efficient and put it at a competitive disadvantage. The opposite strategy of trust without restrictions, which Ananth calls the "kumbaya approach," increases the risk of a data breach. The middle ground is the best, he argues. "We like the trust-and-verify approach."

One-quarter of banks are taking a hard line on devices while about one in 10 have a generous "bring your device to work" policy, estimates Andrew Jaquith, CTO of Perimeter E-Security (Milford, Conn.), a provider of information security services. The remainder, explains Jaquith, make up the "muddled middle" frantically trying to strike a bargain that allows employees to select their own devices as long as the organization can impose security such as device locking and hardware encryption.

For example, iPhone mobileconfig files allow security settings such as remote wiping, Jaquith says. However, in an effort to download non-approved Apple (Cupertino, Calif.) apps, increasing numbers of users are "jail breaking" the iPhone, compromising device security, he notes.

One group particularly vulnerable to attacks on mobile devices is senior management. The act of targeting executives has even spurred a new moniker: whaling. According to Deloitte, executives who tend to have access to more-sensitive intellectual property are less likely than others in the organization to receive targeted security training. They also tend to get their way: Will a security manager be able to insist that the CEO doesn't use his or her iPhone?

Ed Powers, a principal in Deloitte LLP's (New York) financial services practice, agrees that banks need to take a thoughtful approach to smartphones and other devices rather than banning them. "The way we use technology is evolving so rapidly that the answer isn't just to ignore it; the answer is to understand the limitations of the technology, adopt these technologies responsibly, and continue to monitor and evolve our security programs," he says.

[Ed. Note: In an effort to establish security guidance for mobile devices, BITS, the technology policy division of The Financial Services Roundtable (Washington, D.C.), recently launched a Mobile Financial Services Security Assessment Project.]

A Look at Technology

One technology that is become increasingly popular among banks hoping to minimize the risk of data leaving the institution is data leakage-prevention (DLP) tools. According to "Borderless Security: Ernst & Young's 2010 Global Information Security Survey," 50% of financial institutions plan to increase spending on data leakage prevention technologies and processes, an increase of 7% over the prior year.

These tools seek to keep sensitive information inside the organization rather than protect against external entry, explains

ARTICLE—BANKTECH CONT...

David Barton, a principal with consultancy UHY Advisors (Atlanta). Barton notes that USB devices are a particular concern for inadvertent data leakage. For example, a 2010 survey of 500 dry cleaners and laundromats in the U.K. by CREDANT Technologies (London and Addison, Texas) reported that more than 17,000 USB sticks were left in clothes to be dry-cleaned.

DLP products have limitations, says Perimeter's Jacquith. While they can effectively block data such as account or social security numbers from being transmitted to removable media, they are less effective at controlling leakage of competitive or intellectual data.

While DLPs can identify sensitive information leaving the organization, banks must first classify what constitutes sensitive data and where it resides, which in today's environment can be anywhere. With so much data to account for, banks must strategically approach data classification, says Deloitte's Powers, since classifying all data may be impossible. "We're seeing financial institutions focus on targeted data classification and mapping for high-risk data," he notes. "Although tools can automate parts of the classification process, it still comes down to manually assessing the risk of data."

Those banks currently using DLP tools are changing how they use them. "Incidents that used to be noted as a warning are now being blocked," explains George (Chip) K. Tsantes, principal, financial services, for Ernst & Young (New York). "We're also seeing more financial institutions reviewing unusual volumes that could indicate that malware has been installed and is scanning the network."

In a somewhat ironic twist, mobile devices and smartphones--the very devices causing security headaches for banks--are also capable of providing a stronger security platform than what's available on personal computers, says Mercator's Peabody. In addition to holding promise for contactless payments, near-field communications (NFC) chips embedded in mobile devices can be used for multifactor authentication.

Although NFC is not yet ubiquitous--and Apple recently announced that this summer's release of the iPhone 5 would not include NFC--Mercator is predicting that 40 million NFC chip sets will be shipped in the North American market in 2011. "Rather than buying a token generator, the chip is already in the hands of the user," says Peabody. "Banks just have to figure out how to get access to the chip and use it for authentication."

Another technology increasingly used by banks is Security Information and Event Management. SIEM solutions provide the same features as event log management tools but go further with event-reduction, alerting and real-time analysis and typically allow users to import non-event information such as vulnerability scanning reports. SIEM can help find the needle in the haystack, says Chuck Daye, MIS administrator and senior vice president, First National Bank and Trust Company in Chickasha, Okla. (\$350 million in assets). The community bank creates more than one million log records per day. Reviewing those records required Daye to log onto many different platforms to monitor the bank's servers, network switches and firewalls.

First National Bank and Trust uses LogRhythm's (Boulder, Colo.) SIEM technology to consolidate those records onto a single console and to search across platforms, enabling Daye to find the root cause of a problem much more quickly than ever. For example, Daye can correlate seemingly unrelated events such as an outside login attempting to gain access to a server with data leaving the server that could signify a possible breach.

In addition, banks are moving beyond encrypting data in use and in motion and encrypting data at rest as well, notes Greg Rattray, senior vice president for security at the BITS technology policy division of the Financial Services Roundtable (Washington, D.C.).

ARTICLE—BANKTECH CONT...

Implementing Risk Management Disciplines

Although technology can be an invaluable tool in the fight to protect data, technology will fall short unless banks apply rigorous risk management, says Craig Spiezle, executive director and president of the non-profit Online Trust Alliance in Bellevue, Wash. Spiezle cites a Verizon/USSS statistic that organizations could prevent 95% of data breaches simply by following risk management best practices.

Unfortunately, risk management at many financial firms falls short. Although 42% of financial organizations have an IT risk management program in place, only 30% have a program that addresses risks from new technologies, according to Ernst & Young.

UHY's Barton concurs. "At many organizations, there is no difference between highly confidential information or fairly innocuous public information," he says.

It's impossible to protect everything, agrees Prism Microsystems' Ananth, so he and other experts advocate taking an approach that strikes a balance between draconian and laissez faire. "You use the Tower of London to lock up the crown jewels, but it would be ridiculous to lock up loose change," he quips.

Ultimately, this is a challenge for banks' top executives. To paraphrase Spider-Man's Uncle Ben, "With great power comes great responsibility." While mobile devices have empowered employees, employees must be taught to use those devices responsibly, says Prism Microsystem's Ananth.

Yet Ernst & Young's security survey found that an overwhelming majority (92%) of financial institutions consider employee awareness of security to be a challenge. Less than half (45%) of respondents said their firms provide training on the risks of mobile devices and only 34% said their companies provide training on social networking risks.

"Ten years ago, the institution was secure, but all of that is out the window today," notes Ernst & Young's Tsantes. "Financial institutions must step up and educate employees continuously. The biggest department in any institution is the security department because all employees belong to it. Everyone can either enhance or erode security through their actions."

Deloitte's Powers makes the case for deploying good technology such as DLP, but also beefing up employee awareness programs and instituting smart policies that recognize the realities of mobile devices. "You need technology to protect data and minimize the incidence of data loss," he says. "But the reality is that those tools must work in concert with good policies and increased awareness of security throughout the organization."

FOR MORE INFORMATION AND RELATED ARTICLES ON THIS SUBJECT AND RELATED RISK MANAGEMENT / SECURITY ARTICLES, PLEASE GO TO: <http://www.banktech.com/risk-management/231300059?pgno=1>

Related Resources

[Confidently Maximize Virtual Investments with IBM Integrated Service Management](#)
[Managed Security Services versus in-house Security Information Management](#)
[The Future of Database Activity Monitoring](#)

CONTACT

For further information or if you wish to reproduce any of the articles in this Newsletter, please contact : Hugo van Zyl on hugovz@saicb.co.za or Melanie Pillay on melaniep@saicb.co.za