SACS Security Audit and Control Solutions

August 2012

TECHNOLOGY BITES BACK

To catch an iThief…

by Mervin Pearce

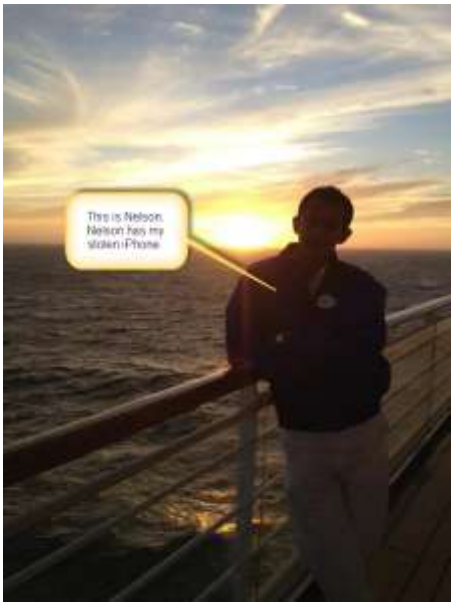
Katy McCaffrey, iPhone was 'stolen' from her during a Disney Wonder ship cruise in April 2012 thinking she will never see it again.

Apple™ products have a feature called the iCloud which allows you to download an application to one device and it is available on any of your other iCloud enabled devices. iPhone has a feature that, when enabled, uploads your images to your iCloud accounts in real-time.

To Katy surprise, photos taken by the alleged thief were being uploaded to her iCloud account as he did not erase the phone or unlink the iCloud account.

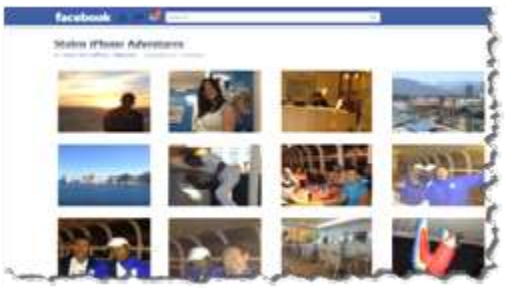
Her friends convinced her to make her Facebook album public for the whole world to see. This link (alive Aug12) is available at https://www.facebook.com/media/set/?set=a.4102695045342.2181863.1221948597

Katy worded her statement correctly by saying 'This is Nelson. Nelson has my stolen iPhone' and not saying directly that he has stolen the phone. Could have been that Nelson bought Nelson also is a given name as she did not know his real name at the time. The phone was recovered, and 'Nelson' was given administrative leave and banned from the guest areas.



This is just one example where technology helps to combat crime although it was not the function of the design.

IN THIS ISSUE



‘Open’ sales

by Mervin Pearce

A 12-year old girl suspecting her sister for ‘stealing’ some of her stuff from her bedroom caught a real-criminal and putting him behind bars. (USAToday)

Hallie Pritchard (12) placed a webcam under pillows in her bedroom to catch her younger sister in the act of taking some of her stuff but an unsuspecting thief was caught on camera going through her stuff and putting some items in his pocket.

Douglas John Calandrella , a former real estate agent, is awaiting trial for burglary after allegedly stealing jewellery and loose change from the Pritchard’s in Orinda. The 46 year old was arrested approximately two years ago for a similar offence.

Police say that during his first offence, Calandrella used keys stolen from lock boxes to steal more than 50 items which he listed on eBay.

How many times have you had people that you do not know in your office or home without supervision? When you create an opportunity, you stand the risk of becoming a victim.

The level of trust we have in a scenario is dependent on experience and the problem with people is that we want to be liked. We then would ‘share’ information that is not required and we can become a victim of your own doing.

As security specialists or auditors it is important to ‘observe’ all the time as at times jokes made by staff may not be jokes at all.

CAN ANYONE BE BOUGHT?

I believe there are three types of users when it comes to fraud. The first type will look for a loophole to commit fraud. The second type will commit a fraud when the opportunity comes along and it seems easy and possibly will not get caught. The last type is a person that commits fraud to make his ‘family survive’

TIPS, TRAPS AND TRICKS
info@sacs.co.za

Skill Level Assessment

by Natalia Pearce

How do you know that your staff looking after your business data has adequate knowledge to ensure that your risk is within an acceptable tolerance level?

Assessment using online tools

A solution that is offered by SACS includes a technological skill level assessment for information security which is done by the user online and the analysis is sent to management on the strengths, weaknesses and possible ways to address any shortcomings identified.

Career path development

Information Security, IT Auditing, Risk Management and more is not ‘just a job’ but a career and it is critical to focus on the correct areas and specialize.

Many certification paths are available including CISSP®, CISA®, CCNA®, Security+, and many more.

A service offered includes on-site assessment of a group writing a skills assessment tests as well as interviews to determine a course of action to develop a career which will benefit the staff member as well as the organization.

To obtain more information send an email to natalia@sacs.co.za requesting a skills assessment brochure.

HEADING 4

Complexity is the enemy...

Complexity is the enemy of security. The lack of knowledge of what you have out there and how it is controlled contributes to the level of complexity.

Add Sidebar Content

With network equipment becoming cheaper by the day with technology making it easier to connect, unauthorized devices may be connected to your network without your knowledge

FAST FACTS

100%

Secondhand network kit we have obtained contained information from the previous owner that could allow a network to be compromised.

80%

Of network equipment has a default password which can be used as a springboard.

FOR MORE INFORMATION

Standard Audit Programs are available to look at some network equipment. Send me an email to see if I can help you with some of them

SEND EMAIL
mervin@sacs.co.za

Often network equipment is accessible by unauthorized staff or guests due to the lack of network standards being enforced in an organization.

Network Perimeter Security

by Mervin Pearce

The invisible perimeter

With the network perimeter being outside a physical location due to wireless access point being placed in your network without your knowledge, your risk is increased also without your knowledge.

Open WAP

A case in point is a 'war-drive' we did using 'NetStumbler' to obtain a list of wireless network access points and their security settings. One of the companies on our 'radar' was a logistical company close to OR Tambo International airport. The access point was found to be open without any security settings and we did get a list of computer names inside the organization. No computer name indicated the organization name and it was safe to use this 'random' list in a presentation.

During a presentation in one of my training sessions I showed a 'sanitized version' of the list and a user in the audience indicated he knows who this list with no information about the client belongs to. I requested that we discuss this in private as it may result in some issues. The user **correctly** identified the client and I asked him how he knows this... He said...'they are our competition and next door to us'

Apart from the fact that the company in question closed the security hole that existed after they have been notified, you could never be assured that some unauthorized client, consultant or contractor has access to your data which should be protected.

Residual data

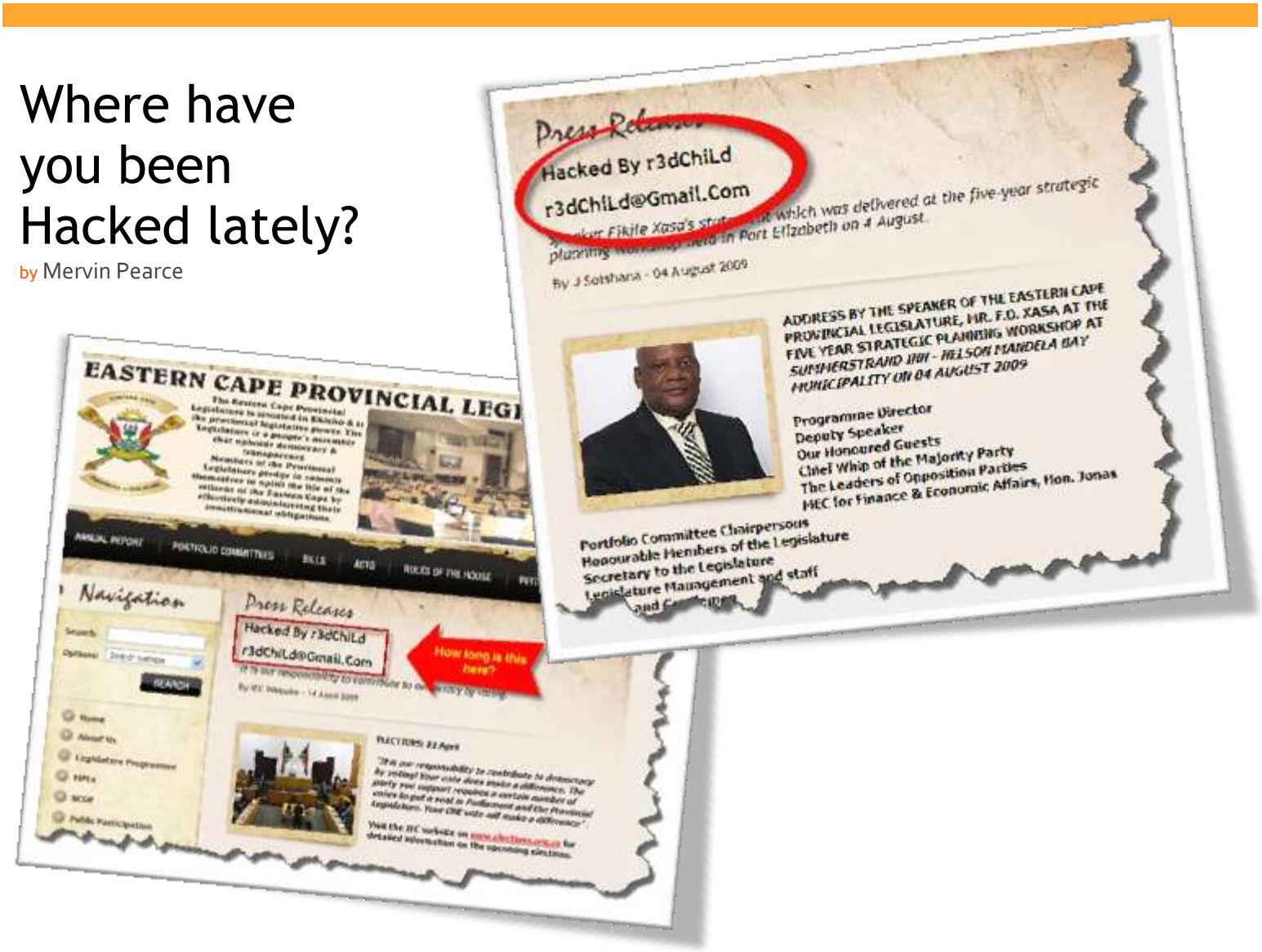
So far every Cisco network device we have obtained for training some of the internal staff contains confidential configuration settings. Information includes network design considerations, SNMP community strings, access and enable passwords.

Solutions

1. Have an up-to-date asset management solution to identify devices that are NOT your register;
2. Staff need to know what is authorized and what is NOT;
3. Have an acceptable use policy which can be used in case of non-compliance
4. Education, Training and more importantly an awareness program is required;
5. Any device that is decommissioned needs to be sanitized;
6. Make sure default passwords are changed;

Where have you been Hacked lately?

by Mervin Pearce



On the **9th of May 2011** evidence was obtained that the website of the 'Eastern Cape Provincial Legislature' which was compromised by a hacker with an alias of '**r3dChiLd**' (red Child). This is a '.gov' owned site which we expect have to be monitored and secured

The image at the article was taken on the 1st of August 2012 which means that since the

identification of hacked content of the government site, there is still evidence of the

compromise. Does this mean that the keepers of the site do not know what they are doing? Are the correct people looking after the site?

There are commercial solutions as well as scripts that can used to monitor your website and notify the correct people to take action. There are NO EXCUSES that can be used in this scenario.

The questions that the organization should pose include:

1. Who is responsible?
2. What is our security stance?
3. What are the consequences for non-compliance?

If you cannot answer these questions then your security is non-existent and possibly only window dressing.

FOR MORE INFORMATION

Identifying hacks is easy but closing them seems not to be important by the site owners. Is this a lack of skills or a 'just-don't-care' attitude?

EXAMPLE OF HACKED DOCUMENT
http://www.eclegislature.gov.za/news_article/52/Hacked_By_r3dChiLdbrbrr3dChiLdGmailCom/04_August_2009

Training courses

by Natalia Pearce

Education and training is critical to improve the productivity of staff as well and to ensure that the organization meet or exceed compliance requirements. SACS has the following courses which range from instructor led to online preparation. DVD or downloadable media is also available.

The advantage of using local trainers is the level of access a candidate has with the trainers post the training session. We keep in touch with all our students with additional training material and other information for as long as they agree.

CISSP

The Certified Information Systems Security Professional is the 'GOLD' standard for information security worldwide. SACS has been developing and delivering the CISSP training locally in South Africa since 2000.

ISSAP

Once you have certified, specialized streams are available and this one focuses on Security Architecture. ***NEW***

CISA

This certification is the one to have if you an IT auditor. Up-to-date materials with interaction with the trainer from training until you write the examination. ***NEW***

CISM

'Certified Information Security Manager' which is from ISACA and covers Security Management as a deliverable maintaining a balance between business and risk. ***NEW***

Bank Fraud Management

With numerous forensic and fraud investigations under our hat, we have developed a training program looking at the users methods of committing fraud along with the controls that an organization have to put in place. ***NEW***

ITIL V3

IT Service Management with new focus on security as an enhancement. ***NEW***

ISO2700x

Information Security Management (ISM) has a standard and it contains many areas of implementation, monitoring and review.

Barefoot IT Auditor

If you an IT person who needs the skills to become an IT Auditor or a general auditor who wants to be an IT auditor, this is the course for you. Hands-on practical work with applicable standard audit programs is included. Report writing skills and

Computer Forensics and Investigation

Hard-core, hands-on covering all aspects of evidence life-cycle from First Responder to forensic analysis requirements. Develop a program to ensure your organization is forensically ready.

Information Security Awareness

Internal online training clips for all kinds of information security awareness, password management, policies and acceptable use.

Delivery methods

SACS has a LMS (Learning Management System) which allows for internal use of the on-line courses along with the ability for management to follow users' progress ad-hoc.

Internal training is available at a special rate which is cost effective but allows for the staff to be more open without fear of talking in front of possible clients or competitors.

AROUND TOWN

Information Security

From Information Security Awareness up to world-class certification programs are covered by SACS Training

Fraud

Fraud Management and Monitoring in financial institutions have become a critical component

Auditing

Covering technical requirements, report writing skills as well as tools to use.

About SACS

SACS was established in 1992 by Mervin Pearce who is still developing solutions and consulting in the field.

SACS has three pillars of solutions which include:

- Training and Education
  - Specialized certification and awareness
- Products
  - SACS Fraud and Compliance Solution
  - ISA Log File Analyzer
- Services
  - IT Audits and Security Review
  - Forensic Investigations
  - Compliance Assessments

Contact any of the staff at SACS via email or telephone.

training@sacs.co.za
info@sacs.co.za
Office: +27 (0)11 913-0041
Fax: +27 (0)11 913-0907

SACS
Security
Audit and
Control
Solutions

http://www.sacs.co.za
info@sacs.co.za