



@jjza's tweetbook

Created by Justin J Williams

(Includes tweets from 05/27/2014 till
05/28/2014)



@jjza

Justin J Williams

living, studying, working in Durbs and Jozi. Information security for Transnet my current challenge. All opinions expressed here are my own.

Durban, South Africa

@jjza's tweetbook

Contains 447 tweets tweeted between 05/27/2014 and 05/28/2014.

Created on 03/06/2014 by <http://tweetbook.in>.

Be a [tweetbook.in](https://www.tweetbook.in) sponsor.

2014

May

27th May, 2014

- 08:36 #ITwebsec about to kick off. Running a few minutes later. <http://t.co/qGCr535XHr>
- 08:40 RT @marinusva #itwebsec where rage against the machine meets revenge of the nerds
- 08:40 RT @telspacesystems We'll be exhibiting at the ITWeb Security Summit (@itwebsec) tomorrow and Wednesday, come visit our stand and get some swag! Stand 37!
- 08:53 Jeremy Maggs kicking off #itwebsec 9th annual event. The post Snowden era will be a key focus area <http://t.co/x3izJ53cwx>
- 08:55 @singe was looking forward to catching up with you and chatting about the Isaca conference and your offer to speak
- 08:56 RT @RankaJ ITWeb's Security Summit starts, over600 people expected #itwebsec <http://t.co/MeKiXdnCTe>

- 08:57 Hello @tallulahlucy :) Looking forward to your coverage of #itwebsec
- 08:58 @singe yes that would be great.
- 09:00 @fakejon setting the scene with an overview of evolution of business and the information security discipline. Treating the disease #itwebsec
- 09:03 A gloomy picture from Target breach. PCI doesn't prevent compromise. @charlvdwalt compliance <> security #itwebsec
- 09:05 Looking forward to @0xcharlie speaking on Car hacking. Is it safe to drive ? #itwebsec Offensive security marches on
- 09:08 What Infosec problem are you trying to solve? Doing things for compliance or to recognize + mitigate a real threat? @charlvdwalt #itwebsec
- 09:09 RT @Liron_Segev Heads up: too much good value from the #ITwebsec summit. If getting flooded here is how to block hashtag: <http://t.co/hBhH3yo5uH>
- 09:13 RT @Liron_Segev #Itwebsec: thats frightening- BadBIOS uses/ could use the PC speaker communicate with other infected pc via sound in frequency we cant hear
- 09:14 RT @tallulahlucy Ross Ulbricht (Silk Road) looks so young. Yet basically a mob boss. #ITWebSec

- 09:16 @tallulahlucy true but no more so than Mark Zuckerberg just chose different paths ?
- 09:19 @tallulahlucy sure though the physical violence aspects seem more abstracted
- 09:23 @abaranov @charlvdwalt They were able to systematically ignore them for a period+still achieve compliance is concerning. False sense of sec
- 09:24 RT @fakejon Phenomenal turnout at ITWeb Security Summit, and some great speakers to come. Going to a good week! #itwebsec
- 09:25 @flaubscher @tallulahlucy More surprising things have turned out to be true.
- 09:26 RT @LenzoManzo #itwebsec InfoSec giant RSA allegedly paid by NSA to deliberately weaken its security in its products #Snowden
- 09:27 Who is the adversary? Do we really know anymore who are the good and who are the bad guys? So much grey #itwebsec
- 09:28 RT @Liron_Segev #ITwebsec: NSA scans 29.21 petabytes of data per day. By comparison size of 10 billion photos on FB is 1.5 petabytes <http://t.co/9mCjyfbQUO>

- 09:29 RT @eversonc @rapid7 here at #itwebsec stand 51 right next to good coffee, come and have a chat about Vulnerability management
- 09:31 Jacob @ioerror up on stage. South Africans understand the context of struggle and domination. We can get straight to the core #itwebsec
- 09:31 RT @RankaJ Keynote: Jacob Appelbaum, @ioerror, tech security researcher, hacker and core member of the Tor project #ITWebSec
- 09:33 The NSA Already monitors and correlates information from commercial VPN providers. Don't think you are safe. @ioerror #itwebsec
- 09:34 RT @flaubscher @tallulahlucy @jjza Interesting. Who's to decide what's good and what's bad? "times they are a changin" - Dylan
- 09:35 A lot of what Snowden revealed was not unknown but Snowden has taken away plausible deniability @ioerror #itwebsec World leaders are liars
- 09:36 RT @LenzoManzo #itwebsec straight to the point: NSA wins in surveillance and big brother tendencies. Everyone else loses....
- 09:40 internet protocols are intentionally being weakened to allow programmatic interception of data #itwebsec

- 09:41 RT @tallulahlucy The book that Appelbaum wrote with Assange: <http://t.co/4sZxEf6iHu> #itwebsec
- 09:43 Every piece of info flowing to and from the UK is kept in buffer for 72hrs to a week so it can be analysed #itwebsec incompatible with law
- 09:43 RT @Liron_Segev @ioerror #ITwebsec: NSA app called X-Key-Score: data is automatically collected from everywhere, sends to a hub which points out red-alerts.
- 09:45 NSA trying to be all seeing all knowing all doing. They believe they are doing Gods work? @ioerror #itwebsec
- 09:46 We have to be able to securely communicate in way where we don't have to rely on others to give us liberty of confidentiality and integrity
- 09:47 Internet protocols are not engineered to give the people confidentiality and integrity of communications. This must change. #itwebsec
- 09:47 RT @ITWeb #ITWebSec Appelbaum: "The problem isn't the NSA - it's that those capabilities exist at all". Standards don't deal with our current reality.
- 09:48 RT @Liron_Segev @ioerror is labelled as "Cast Iron" meaning EVERYTHING he does is monitored forever. Must be "randomly selected" at airports.Alot. #ITwebsec

- 09:50 GCHQ and NSA teamed up and back doored Belgacom equipment because they had interesting clients. ISPs considered fair game #itwebsec
- 09:51 RT @ITWebAfrica Africa lacks computer emergency response team readiness as key countries' CERT websites are offline: <http://t.co/Np3HeECjW7> #itwebsec
- 09:51 RT @Liron_Segev @ioerror #ITwebsec if u do an interesting job eg ISP then u are a target. Vodacom hacked by NSA via hardware as have "interesting" cust.
- 09:53 Did Phillip K Dick inspire the current horror story of surveillance state and create a self fulfilling prophecy ? #itwebsec @ioerror
- 09:56 Surveillance systems built to track Osama bin Ladens of the world. Then realised they can track the rest of us. Now mostly do so #itwebsec
- 09:58 Deep packet inspection/injection : data retention and automated planetary attack - what do you give up to get military protection? #itwebsec
- 10:00 Solutions @ioerror gives : open software, open hardware, crypto, TOR, legal reforms. Not much but best we got. #itwebsec

- 10:01 Trust but verify and then take it and make your own so you can move to independence. Goal of free software is liberty. #itwebsec
- 10:02 RT @tallulahlucy Even if you think it's a good idea for the military to protect company networks there's a historical precedent for this... fascism #ITWebSec
- 10:03 “@enzoparker: Too scared to tweet anything. They are watching you... #itwebsec” they are still watching you
- 10:05 If could make your hardware in country and take back control of the production chain, can have better assurance of what you get #itwebsec
- 10:06 RT @tallulahlucy Appelbaum: Mathematics can stop systems of violence (talking cryptography) #ITWebSec
- 10:06 RT @charlvdwalt @ITWebAfrica To be clear: My comments on CERTs in Africa were a personal anecdote, not an informed assertion of fact. #itwebsec
- 10:06 @p3t3_r lol. Thanks
- 10:11 Legal reforms needed : we need to have power deconstructed not controlled - Bahamas chose legal interception got full monitoring #itwebsec
- 10:12 Need to stop secret wiretapping, not stop wiretapping. Forward secret encryption can provide this. @ioerror #itwebsec

- 10:13 There is no honor among thieves therefore we need use math and change the laws. In our current world can't have security or privacy #iwebsec
- 10:13 RT @Liron_Segev .@ioerror #ITwebsec: mobile phone calls app like RedPhone can ensure secure calls as they destroy the encryption keys after the call.
- 10:13 RT @tallulahlucy Appelbaum uses The One Ring as metaphor for "Lawful interception" laws in SA: no one should control the power #ITWebSec
- 10:14 RT @Liron_Segev .@ioerror #ITwebsec Wiretapping will never stop. But secret wiretapping should. U should be able to go to a judge & ask why u being recorded
- 10:16 Neocoloniast history will be used against African countries. Who built our networks? either Chinese or Americans. Have our keys. #itwebsec
- 10:17 White Americans who build or sell systems seem to be surprised when they are targets or their systems used to do harm #racists #itwebsec
- 10:18 When network controlled by people who don't respect basic human rights will exploit it because they can @ioerror #itwebsec
- 10:19 There is no winning, only a state of continuous revolution. We can move to a place where we can mostly agree. Is no end. @ioerror #itwebsec

- 10:21 RT @tallulahlucy Chair: "How do we win?" Appelbaum: "There is no winning. There is only continual struggle... not to sound like Tolstoy" #ITWebSec
- 10:23 Even open platforms like Android run on a platform slave to a baseband processor which run proprietary software. Not so open #itwebsec
- 10:28 Less than a hundred people globally could analyse hardware and declare it safe. #buzkill #itwebsec Need to open this up. Build capacity.
- 10:30 RT @LenzoManzo There are possibly only as few as 100 people in world qualified to do assurance on hardware...scary how blind trust is #itwebsec
- 10:32 "we track em you whack em" Drone attacks based on metadata. Suspicion <> confirmed guilt. Metadata can be wrong. Not justifiable #itwebsec
- 10:33 Nelson Mandela was considered to be terrorist in many parts of west. Would it have been right to initiate drone assassination? #itwebsec
- 10:35 After @ioerror and @charlvdwalt now we have @csoghoian up on stage. Great lineup this morning. Hard act to follow #itwebsec

- 10:36 RT @RankaJ Keynote: Christopher Soghoian @csoghoian, policy analyst Speech, Privacy and Technology Project at American Civil Liberties Union #ITWebSec
- 10:36 RT @LenzoManzo Story about CIA and drone strikes based on metadata <http://t.co/fPGiUGw9t2> #itwebsec
- 10:39 @ioerror Thanks for an enlightening presentation and coming all the way out to SA to speak with us. Much appreciated.
- 10:41 RT @tallulahlucy FBI director in 1997 believed uncrackable encryption was most evil of evils. Advocated crypt that could be accessed by gov. #itwebsec
- 10:41 RT @LenzoManzo Back to the clipper chip. Reminded of infosec back in the days #itwebsec
- 10:46 Regular people really struggle with security. PGP is almost as difficult to use now as 18 years ago. Incorrect use most dangerous #itwebsec
- 10:48 Just 5 years ago in 2009 the likes of Yahoo Facebook Twitter Google etc were all communicating with users in clear text @csoghoian #itwebsec
- 10:51 Government has coercive power over network providers because of extent of regulation in market. Provides effective surveillance #itwebsec

- 10:54 The shift from HTTP to HTTPS by default in Jan 2010 started by Google made surveillance more difficult. New methods needed #itwebsec
- 10:58 The last year of Snowden reports has pushed US tech companies to drastically improve their use of encryption @csoghoian #itwebsec
- 10:59 Google and Yahoo support server to server mail encryption (tls) but Microsoft and AOL still don't use it #itwebsec
- 11:00 RT @nicocoetzeel Not encrypting your internal network makes it easy for NSA et al to get useful data. Encrypt all your traffic! #itwebsec
- 11:02 Don't forget the Tech Companies are business people out to make money. They have your unencrypted data and will give it to state #itwebsec
- 11:04 Security that is complimentary to business model will be rolled out. That which hurts the business model will be avoided. #itwebsec
- 11:04 RT @ITWeb #itwebsec Google: we couldn't run our system if everything was encrypted, we wouldn't know what ads to show you
- 11:07 Google keeps data longer then it needs so it can provide it to law enforcement when requested. Schmidt 2009 #itwebsec

- 11:10 RT @RankaJ Skype has modified their servers to make it possible for FBI to tap their users - Soghoian, @csoghoian #ITWebSec
- 11:12 Microsoft have given up. They are not going to try give you proper encryption or security on your skype calls or communications #itwebsec
- 11:15 Companies that we trust and rely on get requests from government to be patriotic and do the right thing to fight terrorism + crime #itwebsec
- 11:16 RT @BigConcerts #30STMSA dates postponed to 21 Nov JHB and 23 Nov CPT . All tickets are valid for the new dates. For ticketing enquiries dial 011 759 7215
- 11:19 What worries @csoghoian most? Government mandated back doors - threat of government orders to companies that provide secure comms #itwebsec
- 11:19 RT @MarisaO2 #quoteoftheday from Martin Luther King. <http://t.co/BC9yplhvoV>
- 11:22 Lavabit server 400 000 customers. US government demanded private keys as wanted one user details and would have compromised all #itwebsec
- 11:25 Our threat model has changed. We must recognize that in products we build and services we offer @csoghoian #itwebsec

- 11:59 @abaranov @charlvdwalt Standard issue with periodic audits done at a point in time.
- 12:01 2.6 virus strains detected per second. On average it takes 11.8 days to detect a new virus #itwebsec
- 12:01 RT @Liron_Segev #ITwebsec:57% of cust are not protected from advance cyber attacks, 63% cant stop theft of corporate info, 74% dont trust their sec program
- 12:03 At #itwebsec last year everyone was talking cyber kill chain. This year it's Snowden, NSA and the surveillance state.
- 12:06 Web sense Threatseeker Majority of SA Web traffic stays in the Borders, then to USA next highest percentage #itwebsec
- 12:08 Are significant anomalies between normal & malicious traffic originating from SA. Hong Kong & Algeria come up tops #itwebsec
- 12:11 A lot of your users are targeted when they are outside of the protection of corporate firewalls proxies IDS etc. Awareness key. #itwebsec
- 12:12 Signature less methods of defense required that assess the entire redirect path to deal with current threats #itwebsec

- 12:15 The bad guys are using dynamic DNS, encryption, tor and other methods to evade detection. Need scan/monitor outbound traffic #itwebsec
- 12:17 In 2013 30% of malware used custom crypto to get data out of organisations and avoid detection #itwebsec
- 12:19 We need pervasive and active threat intelligence to secure our systems. Must secure network of one, raise Human Security IQ #itwebsec
- 12:21 RT @ateeeeqkhan AV Firm Avast Shuts Online Forum After Hack Attack <http://t.co/NufE1jluVA> #ceureit
- 12:22 RT @NokiaRSA The FIRST 10 fans to reply to this tweet will WIN double tickets to #CAPSOLive | Thurs 29 May | JHB ONLY @TRACE_Inter <http://t.co/Ry9aXKzJj5>
- 12:24 Could crowd sourced human intelligence help us fight the security threat ? #itwebsec
- 12:28 Kevin Kennedy - Juniper Networks - The idiots guide to destroying a Global 500 Company ... For £500 #itwebsec
- 12:31 RT @LenzoManzo The objective is not build higher walls but to protect companies by changing the economics of hacking #itwebsec

- 12:32 \$2000 buys you malware that can evade antivirus, seek out source code and send it securely back to you. Destroy companies #itwebsec
- 12:37 @Liron_Segev there were naartjies at the tea stand ...
- 12:42 There is return on investment in the malware economy. To limit malware we need destroy the economy #itwebsec Use tech legal and financial
- 12:42 RT @ITWeb Kennedy proposes way to stop malware is changing the economics like we have been with spam, making it less worthwhile #itwebsec
- 12:43 RT @Amethyst_za Design your networks & applications assuming that you have been breached #itwebsec
- 12:45 RT @tallulahlucy Basically the way to combat malware: Make it less worthwhile, more risky for less reward. "change the economics of it" #itwebsec
- 12:48 Belief that after Liberty Reserve was shut down malware economy has moved to Bitcoin. Kennedy argues for regulation of Bitcoin. #itwebsec
- 12:50 Design with breach in mind. Assume credentials are going to be stolen. Figure out how to stay secure in this scenario. #itwebsec

- 12:52 Visit Panopticlick to see how unique your browser signature is. Probably much less so than you think. Over 200 data points #itwebsec
- 12:54 @valdesjo77 @ITWeb_Events most are made available for download a little while after the event. Keep checking the website
- 12:56 RT @LenzoManzo Traditional device-based security is insufficient. Always assume the device is owned...often missed basics #itwebsec
- 13:00 Noise and false positives block our ability to deal with the real threats. Easy to look back but much harder on real time #itwebsec
- 13:02 Can we do something that does away with the noise and brings certainty? Can we lure the attacks to identify themselves? #itwebsec
- 13:02 RT @ITWeb One of IT security's biggest problems is noise -false positives. Don't want to block real customers. How do you know real alerts? #itwebsec
- 13:05 Smoke out malware : fake command and control commands, provide fake monitored files, run fake AV processes for malware to disable #itwebsec
- 13:07 Antonio Forzieri speaking at #itwebsec on Cyber resilience calls for strategic action. Now.

- 13:09 We operate in a Hyper connected rapidly evolving environment with agile target threats. High cyber risk for us. #itwebsec
- 13:10 RT @Amethyst_za Zone based segmentation in data centers are insufficient. Application based segmentation mitigates risk #itwebsec
- 13:13 Lloyd's and the World Economic Forum both have Cyber Security / Cyber attacks in their top four global risks. #itwebsec Cyber is catchphrase
- 13:13 RT @LenzoManzo InfoSec is serious business and we should treat it as such....can't help wonder if we are our own enemies in this regard...#itwebsec
- 13:18 2013 saw a 91% increase in Targeted Attacks. Most happened in Oct-Dec in time for Christmas shopping rush. #Symantec #itwebsec
- 13:18 RT @Liron_Segev The first Ransomware locked your pc and charged you to unlock it. It made \$5 million ! #ITwebsec
- 13:19 RT @tallulahlucy 40 million credit card details stolen after Christmas last year according to Symantec stats #itwebsec
- 13:27 RT @thinusswart Data exfiltration is not rocket science, according to Antonio Forzieri #itwebsec

- 13:34 RT @Liron_Segev #ITwebsec: "if you are faced by a state sponsored attack - you are dead. Nothing you can do. They have more time & money." - Symantec
- 13:52 RT @thinusswart "User education is important ,even if you think it's useless" - according to @Il_f0rz #itwebsec
- 13:52 RT @Amethyst_za Shift the way we invest money to Detection & Response #itwebsec
- 14:49 RT @p3t3_r To summarize the #itwebsec experience: what hackers have been saying for a numbers of years is now true. believe them. they are prophets lol
- 15:14 RT @tallulahlucy Apparently prior to the big breach Target didn't have a CIO or CSO. Now that'll wake anyone up from post lunch brain death #itwebsec
- 15:21 RT @kalilinux Kali Linux 1.0.7 released. Now with Live USB Encrypted Persistence (with optional nuke) mode. <http://t.co/2MFZ5WE2GE> <http://t.co/tML0EcBYxw>
- 15:27 RT @Amethyst_za Focus on the effectiveness of your controls, not just on their existence #itwebsec
- 15:30 Information regulator in terms of POPI expected to be appointed by September and then likely a year from then for compliance #itwebsec #popi

- 15:32 Organizations are going to need to have process and technology to identify and report breaches to the regulator #itwebsec #popi
- 15:33 In the event of a data breach how will organizations be expected to disclose such a breach and to whom ? #itwebpopi #itwebsec
- 15:36 RT @Liron_Segev So far what I see at #ITWebsec: Remember that homeless guy who screamed at you "They are listening! They know everything!" - he was right.
- 15:39 POPI is principle based, not rule based legislation. It's about outcomes and what it aims to achieve. #itwebsec
- 15:41 In POPI you will be held to account for leaks regardless of negligence or not, so there is no escape clause. #itwebsec
- 15:45 In the event of breach an organization must act immediately. Activate incident process, notify regulator, notify individuals #itwebsec
- 15:45 RT @ITWeb Strategic threat intelligence: assessing likelihood of an attack on your company. Tactical threat intel: preparation for attack #ITWebSec
- 15:47 In the event of breach the regulator will want to know what was done to prevent breach and how you planned to deal with breach #itwebsec

- 15:52 Does government get held to the same standard as private sector in the event of a breach? #itwebsec #itwebpopi
- 15:54 Has there been a risk assessment of the implications of a mass traffic surveillance system? On individuals, on police and others ? #itwebsec
- 15:55 @jjza yes everybody even government is subject to POPI #itwebsec
- 15:57 What's the point of government issuing fines against government? #popi #itwebsec
- 15:59 POPI provides the first legal framework for dealing with breaches in an appropriately serious manner in South Africa #itwebsec
- 16:03 First tip for POPI - don't collect information that you don't need or validate #itwebsec
- 16:04 Recourse to data leaks : approach regulator, take civil remedies, regulator can themselves initiate criminal proceedings #itwebsec
- 16:14 Credit bureaus been collecting personal info for years. Will POPI require them to dump the data and restart with permission? #itwebsec

- 16:15 Lack of access to courts and understanding of rights is a challenge to getting POPI to deliver results. Strong regulator needed. #itwebsec
- 16:17 The quality of the regulator is going to be critically important to the success or failure of POPI in protecting South Africans #itwebsec
- 16:18 Credit bureaus are not exempt from POPI. They are going to have to reform themselves in order to continue operating #itwebsec
- 16:33 After the heated debate&questions in panel discussion on POPI staying for Prof Taylor's session on security compromise reporting #itwebsec
- 16:34 The legal obligation to report IT security compromises - Prof David Taylor #itwebsec
- 16:43 POPI condition 7. To secure data, you must evaluate the risk & take steps that are based on the evaluation. No one size fits all. #itwebsec
- 16:45 Identify foreseeable internal and external risks, establish and maintain safeguards, verify effectiveness. Update for new risks #itwebsec
- 16:48 If personal info accessed OR acquired by unauthorized person must notify regulator & data subject as soon as reasonably possible #itwebsec

- 16:49 Who is authorized? Internally? If wrong person looks at something is that unauthorized? Unpacking POPI doesn't give much clarity #itwebsec
- 16:55 POPI doesn't supersede other laws. If another law allows collecting & processing of personal information then it is still allowed #itwebsec
- 16:56 Consent can be obtained in many ways, including through action. Doesn't have to be written #itwebsec
- 16:58 SAPS are exempt from elements of POPI but doesn't mean they can behave recklessly, they must still behave within the law. #itwebsec
- 17:00 If a user/person is granted access but use information beyond what was intended this is considered unauthorized. #itwebsec
- 17:02 CMDB hugely important when you get down to the granular technical requirements of implementing POPI & appropriate safeguards #itwebsec
- 17:04 Every country has rogue elements that abuse the law / lie to judges to get warrants on unauthorized basis #itwebsec
- 17:06 Would you get notified if SA gov hacked your laptop? Depends on how they got permission. Specific court order or broad oversight #itwebsec

- 17:08 Nader Henein from Blackberry advanced security solutions - now speaking on "Your phone is leaking" #itwebsec
- 17:19 Logging into a Whatsapp type app from corporate phone shares address book. No permission from contacts therefore POPI violation? #itwebsec
- 17:20 RT @LenzoManzo Businesses are concerned about making profit. InfoSec should be about addressing business threats #itwebsec
- 17:20 RT @tallulahlucy "Everything that stops you making money is a threat - ultimately information security is about stopping people stealing from us" #ITWebSec
- 17:20 RT @ITWeb If you talk about patches and versions and updates, you might scare Business but they know by now that the sky isn't falling. #ITWebSec
- 17:21 RT @LenzoManzo Why businesses get turned off about infosec threats by Steve Jump....interesting so far #itwebsec
- 17:28 Sounds like Blackberry collecting and keeping a lot more information than required without getting proper permission from user #itwebsec
- 17:30 @jmnzvs imiea number, mail address details etc. Response by blackberry rep described why some needed but not most nor why stored #itwebsec

- 17:30 RT @LenzoManzo Has anyone ever asked how absurd it is for companies to check laptop serial numbers? Data leakage is a bigger problem..#itwebsec
- 17:33 RT @LenzoManzo InfoSec done properly allows a company to take more risks without losing money - Steve Jump #itwebsec
- 17:34 RT @fakejon Reputation damage may not destroy your company, but it CAN destroy your career - Steve Jump speaking at #itwebsec
- 17:36 When it comes to security&personal information. Trust no one. Unless there is full transparency that you can verify. Trust no one. #itwebsec
- 17:37 @SeanReuben72 collect the data and leak it you are responsible and liable.
- 17:39 Blackberry architect their solutions so they are not party to the conversations for BES and let you add your own crypto. #itwebsec
- 17:39 RT @LenzoManzo Rationalise risk against impact to biz objectives before begging for money to splurge in new shiny solutions #itwebsec
- 17:43 @jmnzvs Probably not. Question everyone and everything. Hard to know who to believe when mistruths/lies all over

- 17:44 @jmnzvs NO. Blackberry probably better than android or iphone but no way to prove that. Stopped using BB as corporate support stopped
- 17:48 Blackberry rep got some hard questions earlier. Personally don't believe iOS or Android more secure. Probably much less #itwebsec
- 17:50 POPI applies to businesses. There will be a point when one individual take another to court over sharing of personal information. #itwebsec
- 17:58 That's it for the day at #itwebsec Time for a drink. Further coverage tomorrow.
- 19:30 @evert_smith very true

28th May, 2014

- 08:54 Up now @0xcharlie asking if Infosec better now than 2007. conference - same topics breaches -no better Patches -same Pwn2own -same #itwebsec
- 08:55 It's not fun being in Infosec if everything can be hacked & whether you try hard doesn't make a difference. @0xcharlie is depressed #itwebsec
- 08:56 Security <> compliance. Each victim Mandiant worked with in 2013 was PCI compliant and still were hacked. @0xcharlie #itwebsec

- 08:58 There are still bugs in commonly used code that have been there for 25 years or more before being found #X11 #itwebsec @0xcharlie
- 08:58 RT @Liron_Segev I dig the way the security expert presenters say "I got into security research". That's code for: I hacked stuff #ITwebsec
- 08:58 RT @ianshak Charlie Miller @0xcharlie at #itwebsec 2014: the more things change, the more they stay the same
- 08:58 RT @thinusswart According to @0xcharlie, "Everything can be hacked, no matter how secure you try to be" #itwebsec
- 08:59 RT @tallulahlucy Miller is depressed about state of security: most hackers hack for fun. Companies can't even protect selves from kids goofing off #itwebsec
- 09:01 It is much easier to find one bug to compromise a piece of software/system than to find all the bugs & secure a system #itwebsec @0xcharlie
- 09:02 It's really hard to write secure software and we really don't know how to do a better job at this point. @0xcharlie #itwebsec
- 09:02 RT @tallulahlucy Enterprises can do everything right... then one staff member uses a vulnerable version of Internet Explorer and they're screwed #itwebsec

- 09:03 People buy features and not security of product. Need get product to market, patch later if needed. No way to measure security #itwebsec
- 09:06 Which is more secure: Amazon or Borders? Can we tell? All can do is trust vendor. Can't make buying decisions on sec <http://t.co/Rs2g8TWp4W>
- 09:06 No real consequences to insecure product. If we get hacked because of a poor vendor product we can't sue them. @0xcharlie #itwebsec
- 09:06 RT @nicocoetzeel Problem: there is a lack of consequences for insecurity #itwebsec
- 09:08 When @0xcharlie hacked iPhones through SMS was there stock price dip? No! Just went up #itwebsec #noconsequence <http://t.co/rCGZZuFjnX>
- 09:09 You can never secure your enterprise. Goal is to drive up the cost/pain to attacker so not worth their while. Gov can outspend you #itwebsec
- 09:09 RT @tallulahlucy When Miller managed to exploit iPhone through SMS in 2010 it made huge headlines... But Apple stock went UP #itwebsec
- 09:10 Although government could hack enterprises @0xcharlie proffers that they are not really the attackers you should be worried about #itwebsec

- 09:11 Know your attackers and target your defenses against those so you can make a difference. #itwebsec @0xcharlie
- 09:12 There are no laws requiring secure software. Lobbying won't easily change this. There are no bodies to certify sec of products #itwebsec
- 09:14 Can military help secure us? Vulnerability can be patched or weaponised not both. They can't be trusted to defend us @0xcharlie #itwebsec
- 09:15 Could we outlaw sale of exploits? Problem then ban tool sales. Fuzzers? Scanners? It's already illegal to use exploits. Enforce. #itwebsec
- 09:17 Problem with press. Not proponents of truth. There to get clicks or sell newspapers. Talking about fact is boring FUD gets views #itwebsec
- 09:18 Trying to secure an enterprise? Last thing you should be worried about is whether your tv can be hacked. Headlines distraction. #itwebsec
- 09:19 Enterprise must focus on real threats and avoid the distractions. Stunt hacking and NSA are not the threat. @0xcharlie #itwebsec
- 09:21 It's harder to find bugs now then before. Can take weeks. Researchers don't want give away their time. Choice report, bounty, sell #itwebsec

- 09:22 Hard to fault a researcher who chooses to earn an income vs trying to get cred @0xcharlie #itwebsec
- 09:23 Our security shouldn't rely on a 17 year old kid in poor economy choosing to make "the right choice" - but it does @0xcharlie #itwebsec
- 09:24 Security of products has improved. Less bugs. App sandboxes. Code signing. Anti exploitation. #itwebsec
- 09:25 RT @haroonmeer Stylish & privacy preserving: sequence on @0xcharlie's machine at #itwebsec
<http://t.co/00xnURvLYp>
- 09:26 RT @tallulahlucy Sometimes media gets it right: like with Heartbleed. Miller finds this encouraging. "We are getting better" #itwebsec
- 09:27 RT @ITWeb On the bright side, it's getting harder to write exploits and vendors are starting to smarten up #itwebsec
- 09:28 Bug bounties have improved. Google paid 2 million dollars on chrome. Average \$5000 which is a lot of money on some parts of world #itwebsec
- 09:28 RT @aFREAKaSA @jjza @0xcharlie You should see how many bugs are in Tamboerskloof. #aFREAKaSA

- 09:30 Charlie's conclusion : we are in bad shape but there are some positives #itwebsec @Oxcharlie
<http://t.co/ZEPzPYTnHR>
- 09:32 Up next at #itwebsec @haroonmeer on what the Snowden revelations mean for South Africa
- 09:36 @wildebees what was the vendor response to your responsible disclosure process? They are not quoted on your advertorial site ?
- 09:38 There are lessons from Snowden for corporates , for security folk and for our country as a whole @haroonmeer #itwebsec
- 09:38 RT @Liron_Segev #ITwebsec @haroonmeer : "As good as the NSA is, Snowden walked out the front door with their stuff" Something to think about....
- 09:39 You need to know what you have and who has access to it. Figure our what and who before can secure it #basics #itwebsec
- 09:42 @wildebees erroneous assumption on my part. Apologies. Site doesn't seem to be in best interest of product user community. Your view ?
- 09:45 G20 summit spying was primarily done to gain advantage in the negotiations and South Africa was one of the targets @haroonmeer #itwebsec

- 09:45 RT @Liron_Segev #ITwebsec:"If you think Crypto will solve your problem then you dont understand Crypto or you don't understand your problem" - Chief at NSA
- 09:45 RT @tallulahlucy Something else we learned from Snowden's leaks is that the NSA lacks PowerPoint skills - Haroon Meer #itwebsec :D
- 09:46 RT @thinusswart Something I've learned at #itwebsec: Only secure thing you can do is encrypting your own files before uploading anywhere.
- 09:48 Before Snowden everyone hated on China for hacking &those saying all doing it hounded. Now proven all doing it+China not bogeyman #itwebsec
- 09:49 A surprising number of SA military websites have cloud mail addresses (yahoo gmail etc) for contacts. Problem. #itwebsec @haroonmeer
- 09:50 RT @LenzoManzo Mac Maharaj uses an icloud email fof official gov business.....#itwebsec
- 09:50 RT @Lihle58SR If you using the cloud for anything sensitive then you doing it wrong #itwebsec
- 09:51 What are we saying? Don't use cloud and don't use US products? If so we close shop. We are deeply dependent on foreign skills #itwebsec

- 09:53 @p3t3_r lol. No payment here. Just me my iphone and extra battery pack.
- 09:53 RT @ianshak Haroon Meer @haroonmeer cracking up the #itwebsec crowd by describing the NSA hacking Belgacom while Snowden was walking out the back door
- 09:56 Go and read the secret history of Silicon Valley at <http://t.co/7Dc2vuGEGk> Fascinating insight being summarized by @haroonmeer #itwebsec
- 09:57 RT @nicocoetzee1 <http://t.co/3bSFeWtFzW> - the secret history of Silicon Valley #ITWebSec
- 09:57 RT @Karlouse "@ITWeb: "There are no allies, only interests" - Meer #itwebsec"<--- No honor amongst thieves!
- 09:59 A scary number of US security vendors can have funding traced back to military funding #itwebsec @haroonmeer Not good or bad just a thing.
- 09:59 RT @tallulahlucy Everyone wants to be the next Silicone Valley. But forget military funded birth of the original. #itwebsec
- 09:59 RT @ITWeb Silicone Valley was birthed by military funding and military still funds venture capital. #itwebsec

- 10:00 In South Africa we are not channelling resources to funding research. We are creating technology consumers not researchers. #itwebsec
- 10:02 Auditor general reported in 2013 102 billion rand spend on ICT consultants. Surely some of this could be spent on research #itwebsec
- 10:03 Research funding is not charity. When the companies are taken public the venture capital funds recoup their investments #itwebsec
- 10:05 @wildebees agreed. Lack of mention of any communication leads one to believe that is the case. Ending with a sales pitch more so.
- 10:05 RT @Liron_Segev #ITwebsec:Do this Google search: "site:gov.za *@icloud.com" or "site:gov.za *@gmail.com" - how many official gvmnt officials use cloud mail
- 10:05 RT @nicocoetzee1 FLOSS to the rescue! #ITWebSec
- 10:07 We all use open source, embedded in google apple android etc without realizing it. We must capitalize & bootstrap off open source #itwebsec
- 10:08 @Bitcrack_Cyber can you succeed off a phone or does one need a laptop ?
- 10:08 RT @Lihle58SR We are Ubuntu #itwebsec

- 10:08 RT @Liron_Segev #ITwebsec: South Africa isn't going to build a rival to Skype, but can sponsor the Jitsi project which exists -@haroonmeer
- 10:10 We can't continue with this weird strain of Stockholm syndrome. Feel sorry for NSA due to Snowden leaks? Really? Who do you trust? #itwebsec
- 10:12 We are on a trajectory of continuous dependence on the USA but we don't have to be. We need to take steps to break it. @haroonmeer #itwebsec
- 10:12 33% of apps ask for permissions don't need. 83% users don't pay attention. 42% don't know what means. Avg 41 apps on a phone. #itwebsec
- 10:12 John McCormack CEO of Websense up at #itwebsec on Next Generation security <http://t.co/A57Daw767K>
- 10:12 RT @tallulahlucy Nice quote: the USA is treating cyberspace as one of its colonies #itwebsec
- 10:13 @Biterack_Cyber pity. Thanks.
- 10:15 Jason Jordaan Head of Cyber forensic lab:Special investigations unit of South Africa at #itwebsec relationship bet corruption and cybercrime
- 10:16 RT @Liron_Segev #itwebsec @haroonmeer refers to my story about the Freestate site for R40 million: <http://t.co/P7G3WbUthK> and <http://t.co/haDEQ1k3g1>

- 10:16 RT @zakhanza "If you aren't careful the newspaper will have you hating those who are oppressed" - Haroon Meer quotes Malcolm X #itwebsec
- 10:16 RT @ITWeb "Human beings are the key issue we need to address when we talk about cyber crime" - Jason Jordaan #itwebsec
- 10:18 The entire audience at #itwebsec believe we have a corruption problem and <http://t.co/7h6iKkU0oh> shows it is worsening #itwebsec
- 10:18 Corruption is a part of South Africa. It facilitates cybercrime and organised crime is biggest part of cyber crime. #itwebsec
- 10:19 RT @tallulahlucy "Humans are hackable" - Jason Jordaan, head of the SA cyber forensic lab special investigating unit #itwebsec #socialengineering
- 10:20 @wezside3000 @HornQuentin @wildebees Legal advice says the person retweeting libelous statements are equally guilty as the originator.
- 10:22 Simply phoning users in a government department asking for usernames and passwords to a finance department have up 97% of details #itwebsec
- 10:23 Bad guys identify people on inside and give them a benefit : money, hookers etc for info. Firewalls won't help you in this case. #itwebsec

- 10:24 RT @nicocoetzeel Is corruption in SA an easier way around security controls than phishing? #ITWebSec
- 10:25 @JohanPienaar @wildebees So gave them less than a week & in that time set up a website to commercialize this? My view: conflicted& unethical
- 10:27 RT @dhotman Thanks @haroonmeer for a great keynote at #itwebsec would really like to connect to explore corporate dependancies on public cloud services
- 10:28 How do you mitigate your people risk? Know your people, keep them happy, have ethical tone from top #itwebsec <http://t.co/Ho6POE8D66>
- 10:30 @wildebees @JohanPienaar And the website publicizing the problem with the video was taken live how long before the commercial solution ?
- 10:30 RT @LenzoManzo Beautiful women can be effective honeypots...we hear #itwebsec
- 10:30 RT @ITWeb How do you find insiders? Forget complicated stalking... now we have LinkedIn. "Everybody has a price"- Jordaan #itwebsec
- 10:32 @ortambo_int apologies old tweet stuck in draft queue that suddenly decided to send. Has been deleted.

- 10:35 We need to think outside of tech box and look at all attack vectors including people when trying to defend against vulnerability #itwebsec
- 10:35 RT @Liron_Segev #ITwebsec: A case where someone had physical access to machines in gvmnt & stole over R11 mill. His take: R10k. Banks picked it up not SITA.
- 10:49 @JohanPienaar @wildebees publishing that info along with correspondence history with pastel would in my opinion make it socially responsible
- 10:55 @JohanPienaar you may also wish to add onto your page that disclosure of HR data would be a POPI violation for the company who collected
- 10:56 @JohanPienaar the data and that it's irrelevant whether they knew or not and depended on another party. POPI not yet active but will be soon
- 11:12 Cyber counterintelligence - what it is and what lessons has recent history taught us? Prof SH von Solms + Petrus Duvenage #itwebsec
- 11:20 In 2006 Antivirus was considered an effective method of securing your PC. In 2014 it was declared a useless method. #itwebsec
- 11:23 Reactive methods are needed but not enough. You need to be more aggressive. Prof von Solms advocating going out there&hacking back #itwebsec

- 11:24 We must not just sit back & accept we can only be reactive. We must take proactive steps to defend ourselves. Counter intelligence #itwebsec
- 11:27 Hacking back - preconditions - legality, defense backed, co-operation with the state. #itwebsec
- 11:27 RT @p3t3_r @jjza Big ups to Prof!
- 11:32 We need cyber counter intelligence (CCI) to move from victim to victor - Dr Duvenhage #itwebsec
- 11:32 RT @nicocoetzee1 Lots of talk about "offensive" tactics in counter intel but what is the legal implications? #ITWebSec
- 11:34 Meaning of counter intelligence and cyber counter intelligence #itwebsec <http://t.co/cFCB3XiAfe>
- 11:35 @valdesjo77 waiting to see what they really saying.
- 11:36 To counter we use : defend, deter, detect, deflect, derail, disrupt deceive degrade and destroy. #itwebsec <http://t.co/lnQZ0QtCvp>
- 11:38 Counter intelligence : there are active and passive offensive actions that can be taken #itwebsec <http://t.co/Abgky7bN1O>

- 11:41 @nicocoetzee1 agreed. Kicking the hornets nest ?
Attacking wrong people? Seems much that can go
wrong here
- 11:43 Thin line between low intensity active offensive CI and
Cyber Warfare. Crossing it could be problematic!
#itwebsec <http://t.co/mV5iFmLxf8>
- 11:45 Org's should have capability in each of the 4 quadrants.
Active offensive should probably involve some kind of
law enforcement #itwebsec
- 11:47 Snowdens significant has likely be exaggerated& the
Russians knew most of this already? Sure. But the
American people didn't. #itwebsec
- 11:51 Doesn't matter how small your org is you can invoke
CCI. You don't have to stay a victim. You can be
offensive & aggressive. #itwebsec
- 11:54 Hacking cars via the CAN bus @0xcharlie and
@nudehaberdasher now up at #itwebsec #stunthacking
#distraction #funstuff
- 11:55 RT @LenzoManzo Most anticipated session on car jacking
#itwebsec
- 11:56 Attack scenarios against cars. #itwebsec
<http://t.co/UVxV3FMjMr>

- 11:57 Each vehicle manufacturer uses their own message formats so it takes a lot of time to do this across manufacturers #itwebsec
- 11:57 RT @DFS_JasonJ #itwebsec I had a really good response to my presentation on the relationship between corruption and cybercrime
- 12:00 ECUs control almost every aspect of cars and run a lot of custom code on unusual hardware. #itwebsec <http://t.co/WEMZ4andc3>
- 12:01 Between one Ford and one Toyota find over 50 computers. Doing simple to complex things such as controlling a seat belt #itwebsec
- 12:02 A bit more info about the CAN messages car ECUs use to communicate with each other #itwebsec <http://t.co/fGHjATHhLL>
- 12:03 RT @nicocoetzee1 CAN messages are broadcast in nature. Interesting! #ITWebSec
- 12:04 ECUs have a problem. No message authentication or security on CAN messages. Was developed in 70s/80s. #itwebsec <http://t.co/gnQ5m0sZDa>
- 12:06 Current attacks : what can you do? Or what can't you do ? Can't bypass physical connections (in some cars) #itwebsec <http://t.co/WLosCdD22V>

- 12:06 RT @ITWeb To hack a car you basically just have to mimic what one of the computers in the car could say #itwebsec
- 12:09 There are safety features in place in cars that prevent some kinda of messages from being obeyed. Some can be bypassed. #itwebsec
- 12:11 These guys @Oxcharlie @nudehaberdasher had a lot of fun crashing and hacking cars. Fun and serious stuff at same time. #itwebsec
- 12:13 You can plug into diagnostic or just clip into 2 CAN wires and then send messages on the bus. Lots of places even outside vehicle #itwebsec
- 12:15 Sending CAN messages blew up the inverter because of sending messages that over revved the engine. Never worked again. #itwebsec
- 12:18 The mechanics tool was reverse engineered to obtain the security keys. Super secure XOR in use. My word #itwebsec <http://t.co/88k3dQW5EY>
- 12:18 @DFS_JasonJ thank goodness for research funding. #itwebsec #killaprius
- 12:20 Not a lot of error checking in the ECUs. The engineers didn't expect messages under circumstances so didn't ignore them. #itwebsec

- 12:22 You can lock and unlock the doors in a Prius by sending CAN messages. Of interest to thieves ?
#itwebsec
- 12:24 You can disable the brakes in a ford via messages. Driving at night, turn off lights then brakes. Horrific scenarios. #itwebsec
- 12:24 RT @ITWeb Some scary examples of car hacks: stop brakes working, control seat belts, swing steering wheel #itwebsec
- 12:27 The ECUs can be reprogrammed to send messages even when you disconnect your PC from the CAN bus.
#itwebsec
- 12:28 Strategies to fix the problem. Not so easy. Need real time sensitive messages. Can't afford delays. #itwebsec
<http://t.co/9TJaGhfNKv>
- 12:30 RT @ITWeb Strategy to secure cars: secure remote endpoints, vary messages car communicates in (through cryptography), isolate ECUs #itwebsec
- 12:32 Woefully inadequate response from the manufacturers and automobile associations to the research that was done. #itwebsec #toyota
- 12:33 Conclusion - a layered approach is needed. #carhacking #itwebsec <http://t.co/CncjP83pNz>

- 12:38 RT @dhotman Really enjoyed car hacking session!
Frightening how modern innovations r build on
ancient tech that doesnt cater for modern risks
#itwebsec
- 14:14 DDOS tools being discussed by Mark Campbell of Arbor
Networks at #itwebsec
- 14:18 RT @tallulahlucy Most of the experts in the South
African police electronic crimes unit are women :)
#itwebsec
- 14:18 RT @ITWeb What is the SA police force doing about
cyber crime? Brigadier Piet Pieterse, head of the
electronic crimes unit explains #itwebsec
- 14:20 RT @ITWeb The key focus within the electronic crimes
unit is "de-silo-fication". Multidisciplinary, world-wide
approach #itwebsec
- 14:23 There are compromised machines on the internet with
shell booter DDOS tool installed that can be found with
a google search #itwebsec
- 14:24 RT @ITWeb "We should attend to each and every cyber
crime case, not just the big ones" - Pieterse #itwebsec
- 14:24 RT @dhotman On cybercrime "We need t agree on a
partnership & multidisciplinary approach that benefits
all SAffers" Lieutenant General Dramat #itwebsec

- 14:25 RT @Friedelien #itwebsec interesting to hear what the SAPS is doing with regard to cybercrime...
- 14:28 Commercial DDOS attacks. 4\$ per hour or \$35 for a week. Free five minute tests. Disable your competitor websites. Thriving market #itwebsec
- 14:28 RT @ITWeb Cyber crime challenges: can't use traditional investigative techniques, can't afford to be reactive, limited resources #itwebsec
- 14:31 As a customer don't make the assumption your ISP can protect you. Ask those questions and prepare before you need the help. #itwebsec #DDOS
- 14:32 RT @ITWeb #itwebsec Criminal procedures act let's police do a search and seize operation but needs to be broadened for modern age
- 14:33 You can't trust DDOS service providers. You could buy a service and become the victim at the same time. #itwebsec
- 14:34 RT @ITWeb #itwebsec In electronic communications act there are outlines about data admissibility in court. Processes to be followed or case dismissed
- 14:38 <http://t.co/k5CCtXuzqq> @JohanPienaar your comments on the Pastel response ?

- 14:39 @NevinSP network service providers have data showing attacks on their&their customers networks. Traffic graphs clearly ID attacks #itwebsec
- 14:39 RT @ITWeb There's a tiny percentage of cyber crime convictions in SA at the moment "We are not impacting the way we want to" - Pieterse #itwebsec
- 14:39 RT @ITWeb Pieterse wants better training: busy on a field guide for the police colleges that outlines how to deal with electronic evidence #itwebsec
- 14:40 @JohanPienaar you have communicated with the MyBroadband journalist to point this out ? Article seemed to miss the point.
- 14:42 @mOnk_dot speaking at #itwebsec on breaking stuff : more to come
- 14:42 @JohanPienaar yes. Given this is a clear POPI violation for unauthorized disclosure of personnel information.
- 14:44 @JohanPienaar @mybroadband @TechCentral how about a follow up addressing the real issue of the Alleged Pastel vulnerability ?
- 14:45 @JohanPienaar putting their clients at risk if all the allegations are true. Glad I'm not a pastel customer or trying to secure environment

- 14:47 Hardware is not magic & is easy to screw up. Software people need not make assumptions. Learn hardware and figure out limitations #itwebsec
- 14:53 @NevinSP there are attacks all the time. Firewall logs should be able show something.
- 14:55 RT @dhotman On tackling cybercrime. SAPS & CSIR a true manifestation of partnership for benefit of all SAffers! Excellent work Piet Pieterse #itwebsec
- 14:57 Some really cool Nand hacking being discussed by @m0nk_dot in the context of mobile phones. #itwebsec
- 15:00 Blocks marked bad in NAND disappear from the system permanently. Tools don't detect these sectors. #itwebsec <http://t.co/SQ8irOGDdT>
- 15:01 Using NAND attack you could remotely kill the hard drive so there is no usable space left and it can't be recovered #itwebsec @m0nk_dot
- 15:03 Android phones have a Power Modulation IC that regulates power from the battery to the phone. Can this be abused to damage phone ? #itwebsec
- 15:06 With Sony and HTC upping NAND voltage through kernel changes (two values) no valid reads or writes to NAND and damages it. #itwebsec

- 15:06 RT @ITWeb People want something simple, make it easy for the user to comply or they will find their way around the system #itwebsec
- 15:07 Dropping power values allows us to read NAND but not enough to write NAND. Reboot doesn't change values so freezes phone in time #itwebsec
- 15:09 Using power voltages couldn't fry the Main processor (SOC) but could brick the phone so once battery flat no power ever gets to it #itwebsec
- 15:10 Attacking the main power plane with higher voltage destroyed the phone almost immediately. Too many components to know which died. #itwebsec
- 15:12 Thermal regulators monitor temperature to prevent a phone catching fire. Programme these to only alert at much higher temperatures #itwebsec
- 15:13 so @m0nk_dot couldn't get the phone on fire. Hot enough to melt it and stop it working but not catch fire. Still impressive #itwebsec
- 15:13 RT @JeanneYzelle #itwebsec Collaboration of teams within organisations are important to enhance malware management procedures
- 15:15 Research will be released soon by @m0nk_dot on processor hacking & recovering crypto keys from the fused "ram" inside the devices #itwebsec

- 15:17 If you are doing destructive hacking on processors, cheaper to buy \$10 processors than \$600 phones. More feasible to do fuzzing #itwebsec
- 15:20 RT @FaSmAL An enlightening & informative day 2 . superb presentations by @Oxcharlie @haroonmeer @nudehaberdasher jason jordan. #itwebsec #eskom
- 16:08 @mOnk_dot thanks for your presentation. Really enjoyed it and rather wished you had been going into more detail for the next hour or two
- 16:08 RT @fakejon Maiendra Moodley has taken a leaf from the Machiavellian CIO talk. "If you want to stall a proposal, send it to a committee" :-) #itwebsec
- 16:08 RT @ITWeb Clever RATs piggyback on Internet connection looking like normal web traffic, meanwhile your comp is under someone else's control #itwebsec
- 16:10 Role of the CISO in enhancing information security governance - Andrew Mpofu - internal audit : South African Post Office #itwebsec
- 16:13 How the CISO fits into enterprise governance of Information Security #itwebsec
<http://t.co/nbCO33Md82>
- 16:17 The CISO should not report to the CIO as there is an inherent conflict between the two - Andrew Mpofu #itwebsec

- 16:18 Problems when not optimized structure: absence of checks and balances, security gets in way, lack of resources, inaccurate reports #itwebsec
- 16:24 @m0nk_dot Thanks will try catch you after the sessions. Hope I didn't misquote you too much in the twitter coverage of your presentation
- 16:25 RT @tallulahlucy De Bruyn (SensePost) doing research into RATting found 1100 live command and control servers, 92k victims, 224 in SA #itwebsec
- 16:25 RT @tallulahlucy De Bruyn (sensepost): I was doing all this research into RATting and figured I might as well do a ma thesis & get bang for my buck #itwebsec
- 16:26 Typical functions of a CISO #itwebsec
<http://t.co/FPR5I2NtVL>
- 16:30 Security is essential for compliance. Eg as a supporter for POPI. >>> Compliance does not however ensure security #itwebsec
- 16:31 Compliance risk and security management need to be taken in a holistic manner #itwebsec
- 16:33 @JAndrews2811 No. It is however something that needs further attention to ensure business services can withstand such an attack.

- 16:34 @JAndrews2811 I'm not sure my business partners would approve (the change requests for) such potentially disruptive testing.
- 16:35 RT @dcuthbert pwning C+C servers by @herebepanda (a dark gray research project) #itwebsec
<http://t.co/vo1N2d0Pz1>
- 16:35 RT @ITWeb Prevention eventually fails. You need to be able to detect, contain and respond to threats once on network - De Bruyn #itwebsec
- 16:38 RT @Karlouse @herebepanda "Security is a people problem, not just a tech problem" #itwebsec
- 16:38 Greg Sinclair - Security research for CIOs - enhancing proactive security strategies #itwebsec
<http://t.co/eJvhSze2QI>
- 16:38 @JAndrews2811 Head up security for a state owned entity
- 16:39 More than half a billion records of personally identifiable information were leaked in 2013 #itwebsec
We need POPI ASAP.
- 16:41 @JAndrews2811 some conversations are best not had in public forums. :)
- 16:41 RT @JP_DUPLESSIS_SA #itwebsec certificates and keys must be monitored

- 16:42 @JP_DUPLESSIS_SA any discussion on how this is effectively done ?
- 16:44 2013 attacks : DDOS SQL injection and Malware most common forms of attacks #itwebsec
<http://t.co/BAXXgec7nz>
- 16:47 @JeanneYzelle please do share the key messages with us
- 16:50 72% of weaponised application attacks against Java and Adobe Reader. #itwebsec How are you protecting against these? <http://t.co/FuAHJgnvGh>
- 16:51 RT @JeanneYzelle #itwebsec "It could be that the purpose of your life is only to serve as a warning to others" S. Kreuzsch on system breach.
- 16:51 RT @dcuthbert small business owners feature in @securitea and @nils talk at #itwebsec cc @thebrugq
<http://t.co/zIdnr0qx6f>
- 16:54 96% of java exploits are applicative exploits bypassing native OS level protection. Difficult to defend #itwebsec <http://t.co/m62FYUDJod>
- 16:54 RT @JeanneYzelle #itwebsec An attacker's tactical objectives- maintain persistence and situational awareness @jjza

- 16:55 RT @JeanneYzelle #itwebsec @jjza "Document everything will assist in building a trend over time" S. Kreusch
- 16:56 @JeanneYzelle What types of information being referred to here ? Volumes of info make this very difficult.
- 16:58 The real threat on mobile devices is compromised credentials rather than specific info. Mobiles better controlled than laptops #itwebsec
- 16:58 RT @JeanneYzelle #itwebsec @jjza On daily basis conduct full network scans on critical data ranges.
- 16:58 RT @JeanneYzelle #itwebsec @jjza Scan your environment before your environment is breached. Be pro-active
- 17:01 Vulnerability growth by year shows a leveling off from 2012 to 2013 at around 8300 per year. #itwebsec <http://t.co/7PrBTMQNBs>
- 17:02 @JeanneYzelle thanks :)
- 17:03 Highest proportion of exploits (26%) written to gain further access to systems #itwebsec
- 17:05 RT @JeanneYzelle #itwebsec @jjza Build and test your DFIR toolbox. #beforethebreach

- 17:07 Only 7% of exploits released in 2013 are fully functional attack capable rather than just POC. Trend down #itwebsec <http://t.co/Xfq7ouCEpv>
- 17:07 RT @JeanneYzelle #itwebsec @jjza Secure your VPN. This is a big soft spot in any environment.#beforethebreach
- 17:09 Scary stat. Number of vulnerabilities reported with no patches available down from 45% to 26% in 2013 #itwebsec <http://t.co/2St9r7vlrU>
- 17:09 RT @JeanneYzelle #itwebsec @jjza Focus on Egress filtering - traffic going out of your network.
- 17:10 Key conclusions : don't forget the basics, social defense needs socialization, enhance proactive measures #itwebsec Greg Sinclair IBM
- 17:11 RT @JeanneYzelle #itwebsec @jjza Maintain traffic logs for vpn so you can see what hacker was accessing or attempted to access #beforethebreach
- 17:15 RT @JeanneYzelle #itwebsec @jjza Outlook Web Access provides access path for hackers to brute force your network
- 17:15 RT @JeanneYzelle #itwebsec @jjza Logs are your "breach flight data recorder" Decide which logs you need and store in a safe place.

- 17:18 RT @JeanneYzelle #itwebsec @jjza Protect your keys to the kingdom - AD(Active Directory) #beforethebreach
- 17:19 RT @JeanneYzelle #itwebsec @jjza Harden service accounts in AD. #beforethebreach
- 17:23 RT @JeanneYzelle #itwebsec @jjza Do annual pentesting. Change pentest companies often #beforethebreach
- 17:23 RT @JeanneYzelle #itwebsec @jjza "Hack yourself" Educate yourself in attack techniques #beforethebreach
- 17:26 What does it mean that IBM is named as a strategic partner of the NSA in the Snowden documents ? IBM rep can't comment #itwebsec
- 17:26 RT @JeanneYzelle #itwebsec @jjza Document your incident management process #beforethebreach
- 17:27 If IBM found USA or Canadian government hacking into customer systems would this be disclosed ? IBM rep no comment #itwebsec
- 17:39 RT @JeanneYzelle #itwebsec @jjza Being breached creates awareness for the importance of information security

- 17:50 RT @GarrethBenton Watching those guys from MWR turn Nedbank's PocketPOS into Flappy Bird was the highlight of my day! ▫ Very very talented guys #itwebsec
- 17:51 And that's the end of another successful #itwebsec look forward to another next year. @tallulahlucy
- 18:03 Thanks to @m0nk_dot @0xcharlie @nudehaberdasher @haroonmeer @ioerror @csoghoian for making #itwebsec what it was. Hope you enjoyed SA.
- 18:50 @DFS_JasonJ @dhotman who would be the right entity to undertake such a review ?
- 19:00 RT @haroonmeer Thanks for all the kind words on my #itwebsec talk. We will upload the slides soon.
- 19:03 @haroonmeer Was good to hear a more South African perspective with more tangible positive steps the country can take instead of just ...
- 19:04 @haroonmeer throwing up our hands in despair and blaming a lost cause.
- 21:55 @tallulahlucy Always a pleasure :)
- 22:00 @Liron_Segev @tallulahlucy Intention to inform rather than induce jealousy. Bad enough sitting listening to a presentation knowing the

22:00 @Liron_Segev @tallulahlucy better choice was the session next door. At least know which ones missed worth downloading to listen later.

22:41 RT @thorsheim Now printing all docs stored with Truecrypt, then deleting files. Try malware backdooring my paperstack bitches!

22:41 RT @whitehatsec What just happened to truecrypt? #IsTrueCryptAuditedYet <http://t.co/fGGGARj517>

@jjza's tweetbook

Created by

tweetbook.in