CRN TECH

SEARCH

Features | Galleries | Webinars | Events | Magazine | Newsletter | Subscribe

Home > Features > Technology > Security > CRN roundtable: The changing shape of cyber security

CRN roundtable: The changing shape of cyber security

By David Binning on Aug 8, 2013 10:27 AM
Filed under Security

Like 5 Tweet Comment Now

No target is too small in a connected world.

Attendees

Craig Nielsen, senior director, Channels and Alliances, APAC, McAfee Inc

Sean Richmond, senior technology consultant, Sophos A/NZ

Aviv Abramovich, director of engineering, Check Point A/NZ

Peter Sparkes, director managed services, Symantec A/NZ

Sanjay Mehta, managing director, Trend Micro A/NZ

Neil Cameron, managing consultant, Bridge Point Communications

Aaron Bailey, security practice manager, Dimension Data A/NZ

Keith Price, director, Black Swan Consulting

Part 1 of this roundtable ran in the August issue of CRN. Part 2 starts on page 7.

Part 1

CRN Small organisations appear oblivious to the fact they have assets of interest to criminals. Intellectual property, money in bank accounts, customer contacts. What do we all see as the key implications for this, in particular the opportunities presenting themselves for resellers to help guide their SMB customers?

Keith I'm trying to understand why we are no more secure today than we were last year or three years ago or five years ago and we're always one step behind the bad guys. We need to start approaching the problem a little differently. SMBs have increasingly become the victims. Yet many continue to believe attackers aren't interested in them.

Yet they've got bank accounts, they've got some intellectual property, they've got maybe some credit card debt, depending on who they are and what they do, and they also have computers that can be used as 'bots' to attack other people and spread malware, and so that's a big issue as well. They are definitely a target.

Something I want to talk about later is my concept of the 'cyber kill chain', which is all about the importance of security architecture in protecting your information assets, regardless of how big you are.

CRN With the big imminent changes to the privacy laws, clearly there's going to be a massive compliance challenge. What are we seeing around the table in terms of both that challenge and the opportunities for you as vendors and resellers being trusted advisers to your clients.

Craig We recently surveyed 500 Australian organisations, particularly around the Privacy Act and the changes, and we balanced it. We had a quota for different segments and size of organisation, so we really wanted to get SMB, commercial enterprise and different verticals. Out of that survey 59 percent of Australian organisations said they didn't fully understand the Privacy Act. That's quite staggering. We as vendors, and the channel have a massive opportunity and challenge to communicate the impact on to our customers and to start preparing them. When you're

Tags

mcafee, symantec, trend, micro, check, point, rsa, black swan group, keith price, dimension data, bridge point communications

Related Articles

Datacom secures cloud with Trend Micro

Dimension Data appoints new head of outsourcing

Boycott planned for RSA security conference

John McAfee: "I've been begging them to drop the brand"

Breaking Stories

Amazon is your "ally", says Citrix

Melbourne channel manager's "bring-your-own" CRM hits USA

The long search for Microsoft's next CEO

Apple's new Aussie store to "materially impact" Next Byte

Ex-Heathrow IT head brings client-side clout to Perth reseller

Latest Comments

Polls

Which hyped technology is the biggest opportunity for the channel?

○ Flash storage
○ 3D printing
○ Apps
○ The internet of things

VOTE

view previous polls »

CRN Magazine

talking specifically around SMB, the threshold in the Act is organisations who do over $3 million annually

That actually cuts into a large portion of the SMB market. The other issue requiring attention is the fact the compulsory notification legislation didn't get through. That will be important legislation to close the loophole on what you need to do and what happens if you aren't successful in doing it.

CRN Why do you think then there's that lack of awareness if it's been so prominent in the media. Do you think it's a case of companies being afraid of it, or is it being badly communicated by the government? What do you think is the issue?

Craig Security is a massive issue in organisations and it's not siloed in one part of the business. If you think of a lot of this personally identifiable information, where it actually sits, a lot of that might sit in a marketing department, not necessarily under the governance of the security team. Internally, the issue companies have is getting a consistent framework and policy framework across the organisation. Generally the breaches and failures don't sit in the middle, they sit on the edge.

Neil I completely concur. I work in the GIC space on a day to day, minute to minute basis and for a lot of my clients, the challenges they find are just that. Where is the data, where does it sit? When I walk in and say 'tell me about your environment', they say 'well really that's why you're here'. And how on earth can I quantify what it means to that organisation? I suppose really educating the organisations in question. And with the Australian legislation where it is, one of the challenges I find is that I get executives turning around to me and saying 'why should I comply?'

"I don't have to in the sense that there isn't an obligation for me to state that there's been a breach in my organisation, so I'm good to go, so why should I invest X, Y, Z in going down what sometimes can be an expensive compliance avenue?

CRN Do you think that fact the data disclosure act is yet to be heard in the senate is contributing to complacency within the business community?

Neil Absolutely. I think there needs to be a lot more effort to educate people to say 'this is important' and how do we compete globally as well. You know you've got other countries who are basically ahead of the game, shouldn't we be leading from our side as well?

Keith One of the drivers of the legislation was to help get it up for that exact reason. There were three primary reasons and that was the third one to get it up to there, so we could get it up to other OECD countries levels.

Neil Don't you think Keith that the missing component is that you must release the fact that you've had a break. Otherwise we are going to continue in this 'washing machine' effect.

Keith The Commissioner clearly said that self-reporting doesn't work. So they're going full speed against that.

Sanjay I come from the US which is probably one of the more heavily regulated places, but I can tell you that if you try to compare Australia to other nations, while we may not have the laws and regulations and the breach and notification vocation acts and everything else, the fundamental problems haven't changed. If you look at the US, there's all these entities coming down and saying now that cyber risks are a part of a business operation and should be looked at that way. Has the threat really changed or are companies any more secure or small or medium sized business more in tune to dealing with the problems? I'd say that answer is no, because you now have to disclose that you were breached, but nobody is necessarily disclosing how they were breached to try to help other similar sized businesses.

So I agree that prescriptive is a great way to go and it helps particularly under-skilled or under-staffed businesses get a recommendation as to how to deal with the problem, but fundamentally the problem hasn't changed in fifteen years.

Craig Possibly one of the issues on that is that consistently this topic isn't hitting the boardroom table. It remains an IT compliance risk. It's not really getting the mindshare in the boardroom that it needs.

Sean Compliance is often seen as a technological problem, something to be dealt with, not across the whole business and so it doesn't get the attention it needs. When you're comparing the cost of doing nothing to the cost of doing something, and the cost of doing nothing is not visible on the balance sheet easily, and it impairs the abilities and I think the partners more than the vendors have to be the trusted agents in there, because they are the people who, especially in the small to medium range, know the law. Around about 2000 the awareness of the Privacy Act was much higher, because it was new, and now it's often seen as 'well we've got somebody looking after that we think' so there isn't the attention to it.

CRN Sean you recently gave a very damning assessment of the SMB space in terms of their security awareness, but it seems as though we're saying the awareness of security issues in the enterprise is still lacking, so what chance do the SMBs have?

Sean If you're running a small business, you have to be looking at what the business is doing, and that has to be your focus if you want to survive, if you want to make money. If you don't have the ability to employ specialist security staff, and let's be honest, no small business has that as their priority, unless they are specifically dealing in military or law enforcement, then it has to be an 'also ran' to the overall business model. The ability to provide managed services goes a long way towards that and I think that's going to become something that people rely on much more in that small space.

CRN That's presumably the big opportunity for systems integrators and resellers right? The SMBs don't have the money to hire the specialists internally and in comes the channel.

Aaron I think that a lot of the hype around Privacy Awareness Week was really focused on the repercussions and the fines aimed at individuals in the organisation. What we try to achieve is a pragmatic way to educate our clients. We have four key principles in the way that we go to market. It's principally around visibility, awareness, protection and agility. There are multiple ways, controls, tools and indeed consulting services that are available as a cost effective way to gain more visibility into the actual threats.

The personal information or data in general needs to be valued and classified. There's a lot more value in health records for example. Or tax file numbers compared to marketing database that just has names and email addresses. By educating customers to get some visibility into the real threats and business context, they actually have awareness of what the real risk is to those assets, and they can make an educated decision on how to protect them.

CRN We're obviously talking about a significant auditing task.

Aaron Yes, and we have 160 security staff nationally, about 25 of those are focused on consulting. We do government risk compliance and consulting against standards. The OECD actually released a decent practical guide that had a number of questions for clients to self-assess. I understand that a lot probably won't read it, but they should certainly go through the questions. I think it's an opportunity for the channel to actually take those and package those into a consultative approach and help them on that journey.

CRN How good a job would you say your partners are doing with that?

Aaron A reasonably good job. Certainly during the Privacy Awareness Week we invented a Privacy Impact Assessment – I know of at least one of our partners sitting at this table who was partnering with a legal firm as well to provide a similar privacy impact assessment type, and that was all effectively built and launched through Privacy Awareness Week, and so I think there is a fairly good job being done.

Keith My research has focussed on the concept of situational awareness, and that's what we don't see with a lot of SMBs; the real situational awareness that they have about why they would be a threat. Managing compliance is really just a risk and certainly it's an operational risk and back to Sanjay's point, that's absolutely on the operational risk side that we would manage IT risk and information security risks.

There is a lack of general situational awareness in a classic security sense. Just like when you walk down the street at night, that situational awareness that we have to be aware of the threat, where you're vulnerable, who would want to attack you, how they're going to attack you, what they're after. Those are the things that I think a lot of people that we're talking about just don't do. They just don't do these basic fundamental things.

CRN So what's the answer? Do you use fear to make them more scared?

Craig This is not core business for SMBs, so there is a massive opportunity for the channel and managed service providers to provide that situational awareness to their customers.

Sean That understanding of what makes you a target is very, very low. Attackers are not specifically targeting every business, but there's a huge amount of opportunistic attacks. The price of a compromised PC is a saleable commodity with about 30 or 40 different uses, depending on what you're doing, so you can commoditise the infected machines, but also if you're part of a larger supply chain, you can be a target. No-one's too small to be a target, but not everyone is a target. If you're a contractor working with somebody developing a new building in Canberra for instance, and you're a small construction firm, you may be a target even without being aware of the fact that that makes you a target.

Keith Yes, like attacking a lawyer, because they have a back door into BHP or some other client. That's exactly how they operate.

Sean Yes, exactly attacking a monitoring firm who is running a campaign for a new business in competition with someone else may make them a target.

Sanjay The other thing that's changing is a lot of folks aren't aware of how simple the mistakes can be, right? Conducting research with Deakin University we discovered one in eight IP addresses in Australia now get malware on their website every single day. So these are innocent users going out browsing websites they think are okay and roughly 13 percent of them are going to places where they're getting malware. If you then link that to what we all know, the security professionals and to phishing attacks, and how they're using LinkedIn profiles to figure out information and everything else, you're in big trouble right, and when people hear 'cyber security, and situational awareness' and all these other things, it sounds big and complex, but the fact is that the mistakes are the most basic things.

Keith Indeed. It's the same mistakes about access control, about not updating and having malware, and having networks with the hard crunchy shell and all these sorts of things.

CRN Like only deciding to lock the doors once you've been robbed.

All Yes.

Sanjay This wrestling with BYOD, as if the act of taking the device outside the corporate walls is new. People have been doing that with their laptops for decades.

The form factor is different and you can hold it to your head, so it's got to be different. But when someone leaves the organisation, the first thing we do is 'Bob you're been a great employee, why don't you take two hours, clean up your laptop and any personal photos etc' and give it back to me. It's ridiculous. That's BYOD every single day of the week.

Sean Effectively you have that chance for removal of data and external things. With cloud services, especially, that's far more common.

Aviv We surveyed 3,000 customers, and collected data from all sorts of places around the world including Australia. We found over 60 percent had been targeted, have a 'botnet' an active botnet in their network (over 60 percent worldwide). And Australia is no different. Companies reported BYOD brings more risks into the environment.

Going back to regulation and legislation, it's there to set a minimum bar and maybe raise awareness. But from what I've seen, the greatest inhibitor was that it was too complex, or it is too complex to comply with regulations, be it PCI, SOX, DSD35.

Some of them are just recommendations by the way. They're not mandated, and it's too complex for organisations to comply – even large organisations who can actually afford it, it's costly. And some of them actually take the stance, 'I'm willing to take the risk, and I'm willing to pay the fines – it's cheaper to pay the fines than it is to comply with regulations"? It is a practical business decision that happens every day.

And as Sean stated regarding SMBs there's a lack of knowledge; lack of expertise. We all know security is often perceived to be a very complex topic. It's up to us as vendors to step in and resolve that and make the compliance effort easier. This way even a small business can comply and make sure that they at least adhere to the bare minimum.

CRN Are you suggesting that the privacy legislation is poorly designed, another piece of badly designed Labor policy?

Aviv My view is that the legislation has obviously been impacted by a lot by politics and other factors that might be outside the body of the legislation itself, but I think that asking the government, or relying just on the government to solve these things with very sophisticated legislation is probably not the right way to address it. It's a combination of legislation that raises awareness. In my view, the main benefit of the privacy legislation is to raise awareness. Obviously the more penalties there are, the more people are aware that as Greg mentioned, it comes to the boardroom level. If a CEO can go to jail, yes, it becomes a CEO problem – and in some countries the CEO can go to jail. That aside, I'm not saying if that's the right way or the wrong way. Awareness is the key here, making businesses aware and making it easier for them to actually do something about it.

Sean Does anyone here at this table think that actually complying with legislation equals security?

All No.

Sean In the US Sarbanes Oxley compliance was seen as a lot of work to comply with and so the act of complying became more important than the actual goals you are trying to achieve to be secure. I'm not sure. The legislation as you say, helps raise awareness and makes it something that's safe to talk about at board level.

I advise my clients that being compliant is not being secure, but if you're properly secure, you are already well along your compliance ride, and therefore we turn it around. A few years ago it was all about compliance, which we now realise is an operational risk. You can decide the extent to which you want to be compliant and what is the risk of fines that you might have to pay. But if you turn that on its head and say we should be thinking more about being secure, and then you're going to be able to tick the most important boxes. The second point is that one of the real benefits of the legislation in addition to awareness, is that we really don't know how bad it is yet. As soon as we can get people reporting, we might get to understand how big of a problem this is for Australia. Right now we don't really know.

Maybe three years from now we can probably get an idea of the magnitude of the problem, then that will be an awareness opportunity there, no matter how big or small it is.

CRN How close are we to that level of awareness do you think?

Sean Without breachin we don't know how many companies over this three million size point. We know if we do investigations and consult with particular clients, but who here would know the magnitude of the problem in Australia? If you can't measure it it doesn't exist.

Sanjay We find over 90 percent of the networks have malware on them in some shape or form, so it's hitting everybody. It's there. Now, if we go back to the role of government, an interesting role it could take is where they're already spending a lot of money to understand problems to protect themselves, but also then reach out to say 'here are the types of attacks that are coming towards Australia, and here's how we recommend that you protect your business'. As opposed to 'comply comply comply', you don't really understand what it means, and you may end up getting more secure by actually flipping that on its head to ensure security research. The US recently announced over the last few months that they've selected the organisations that are important to national security and have said 'if we believe the threat is imminent we will inform you'. So all the small businesses raised their hands and said 'hey we pay taxes too, why don't you value me when you value everybody else?'. It's a legitimate argument, but the theme is the right theme, that we protect our borders and protect our shores and everything else, but why don't we protect our information assets in that same proactive sense?

CRN Sanjay, you recently stated there had been incidences whereby a certain malware had appeared only in isolated cases in the US yet seemed to spread everywhere in Australia. Could you expand on that for us?

Sanjay Earlier this year there was an outbreak that hit a service provider here in Australia. We reached into our global operations - where we look at about five terabytes of data every day - and said 'what's going on?' and for that particular attack, we'd seen it 2,000 times in Australia over a two or three day period, and 50 times in the US. Was it targeted to some business in Australia? No. Was it targeted at an area of the world that has a preponderance of small and medium businesses, because it's a soft underbelly? Absolutely.

CRN That's a very frightening reality for Australian SMBs. The smartest evil hacker minds in the world have got onto the fact that there's a whole bunch of companies in Australia that have very poor security policies, and they're going after them. There is a scary couple of years coming up possibly?

Sanjay The flipside of that is we do research on where the attacks are coming from, and they're not coming from here. But if they are, Australians are absolutely brilliant at acting because nobody is attacking them.

Keith The US is a top attacker country, but why? Because they've all got massive bandwidth right (massive connectivity), and connectivity, lots of computers there, and that probably contributes to it.

Sean We did some research last year looking at the threat exposure rates based on PCs and Android; We looked at the threat exposure rate in most of the developed nations where there has been a lot of infrastructure like the UK, Australia, US. There your threat exposure rate is higher with an Android handset than it is with a PC. But in Brazil, China and other Asian countries, there is a lot of pirated stuff. People don't patch as much which increases risks for PCs. So it's a strange situation where you solve one problem and you might not be paying the same attention to another problem.

Sanjay We did some research in the consumer world and consumers believe that their tablets and other devices are secure because they use a PIN.

Sean That's better than nothing – locking your phones.

Sanjay Yes, it's much better than nothing but they would never do that in the PC world. So they've chosen good solutions from everybody around the table for that, but when they go to the Android world, suddenly they figure out 'as long as it's secure for my two year old to log in, I'm good' ---- and we all know the uptake of internet security on tablets compared to that on PCs is still relatively pathetic. It's getting better, but still relatively pathetic.

CRN Sanjay, you said earlier the supposed BYOD revolution is a bit overstated and people would take gear with them in the past, but it's the connectivity and downloading of the apps which is creating massive security headaches presumably for your customers?

Sanjay Yes, I think if you look at what's changing, it's the types of applications that are being accessed, and growing exponentially, and the importance of those applications is growing exponentially. At the same time you have the types of devices accessing those applications which is growing very rapidly, and the pipe whether it be NBN or anything else connecting those two things is also growing exponentially. So those things working in concert have really made the threat landscape a lot more scary than it was, but fundamentally an endpoint is still an endpoint. With your PC, your android device, if you know what the user is trying to do, if you know what applications they're trying to access, and what data is sitting there, the type of endpoint doesn't really matter.

Sean I agree to a certain extent that the information is the important thing that's on these devices, or travelling to those devices, and that's what you need to look at securing. The situation for most admins to get their head around is that you are constrained on these modern consumerised devices which have no concept of a user as such. If you are holding it you own it.

Aviv If we continue that thought we will pretty much reach a conclusion that that has been exacerbated by the adoption of cloud services, and storing your information actually off the device, whether it be tablet, or PC our information actually now exists somewhere else in some nameless, faceless data centre, and you don't know who owns or runs it. Definitely the key challenge will be how to protect the key asset which is the data that you want to store and want to protect. How do you lock it to the individuals that needs to access it – be it on the cloud or on your tablet or in your own organisation?

Keith I would like to envision a world where you have no information on these devices. Everything stays in the data centre; you access it and nothing gets downloaded. If it gets compromised there is no information there, and then you can have the administrator go in to wipe the device, and that's really how I would be talking to clients. Your managed services would be much more secure than your typical SMBs own network. They can use Australian based-hosters so that if there's issues about not knowing where data is we can actually bring that back depending on the data. We should be thinking about the problem that way.

Sean A lot of people assume cloud services provide security but security is often excluded from terms and conditions so you do have to watch that.

Keith We are seeing that starting to change slightly, although customers are of course paying more for it.

Sean I'm a big fan of encryption everywhere. If you're a small business or a medium business or an enterprise and you're using cloud services you should be holding on to the keys, encrypting the stuff that's going up there. It provides you with huge safety as far as being able to say – even as mandatory breach legislation comes in – 'well the data was encrypted' and you don't have to report it, so no worries.

Sanjay With small or medium business, you shouldn't assume your cloud service provider is secure, but it may well be more secure than you believe.

Sean I'm not saying they're insecure, but terms and conditions don't really specify security. So their hosting will be more secure probably.

Keith By the same token, there's not a single security vendor product in that SMB's network with the vendors backing it either. No security vendor says 'if you're hacked we're going to pay you'. There is a company in NZ offering 'Hacking Insurance'. I was at a risk insurance manager's conference a while ago, and they talked about cyber insurance in the US. One point made was that cyber insurance was mostly to get access to the team of people who know what to do when you get breached, who to notify and how to do it, the instant response, rather than getting paid out because you got hacked.

Aviv Cloud services represent a significant opportunity for small businesses, particularly those seeking to dramatically improve their services. But I think the security will be embedded in whatever product they're offering because in general small business just expect it, and we should expect it as well, that security is part of that service. I totally agree with you on threats and countries and the access to broadband infrastructure. We see that time and time again. I'd also point out most Australian companies I'm dealing with already have data overseas, so I think that that has already happened. Even if they don't know about it, the cloud, they will have some sort of data overseas.

So the use of things like encryption, where you control that data, even if that data is in some jurisdiction that you don't know about, is quite important.

CRN Is there not a feeling amongst some of your customers with regard to security as a service, is there a bit of a trust barrier for companies you perceive, having your security managed in the cloud – given that there is a degree of uncertainty about the cloud period – in offering security in the cloud. It strikes me that some customers might be uneasy about that.

Keith I would say that there has been a change in the market. About five or six years ago I saw probably 50 percent of customers saying 'no cloud security, I've got to keep it in house, I've got to control everything'. I don't see that any more.

Aviv A lot of customers are realising that by using online services, you actually get to benefit from the experts and they often get a bird's eye view of attacks and threats coming from multiple customers, and they can correlate that and collect this data, and come up with some really intelligent decisions and mitigation steps. A customer trying to cope with that themselves may not have that same view.

Aaron On the sort of questions that you can ask our providers I agree that most have a key policy that says that the 'responsibility of securing the data is the clients', not the cloud providers'. Typically their key responsibility and what they actually do, is to protect one client from the other. They literally separate the tenants and once they give you your computing power, it's up to you to use it. There are some elegant solutions, in order to encrypt that data and maintain control of that data, and we should be educating clients about that.

Keith I agree, because you can't delegate accountability and it always resides with the customer to do it. Email is a really good way to start in a cloud based service, because it's already clear text going where you don't know. So it's a really good way to get in. The next thing may be to use development environments, where you shouldn't be using legitimate data anyway. You can start it up and down to let people get familiar with that while they start to get those relationships going, and learn that way. Then again there are some things you never put in the cloud.

CRN That brings us full circle to the beginning of the conversation. Do you think small businesses even understand what is most important in terms of their information?

Aaron No, probably not. There's a new service that can actually teach you what the value of your Gmail account is, for end users and consumers. I don't believe I know about a particular service certainly online that does that for SMBs and mid-market. That would certainly be helpful. But I think that started to come about for consumers, because usually people have a reasonably complex password, and then usually they use that password on a number of different services. The service actually scans the contents of your Gmail account, and through that it knows what automatic emails you're getting for a number of different services. Each of those is then quantified in terms of how much money a party could actually make out of that, and it gives you a value of what your Gmail account is worth. An approach to be able to quantify for a client the types and the value of their data is key.

Craig And we've got to figure out a way to educate SMBs on this. As we move to the cloud think of the life cycle management of the data, or passwords, or access. It's really easy to get stuff on the cloud. We thought about how we secure it, and we talked about encryption on the cloud, but have we also thought about how we get it off the cloud if and when we want to do that, and that is an area where I think we really have to create some really simple solutions for SMBs and our channel partners.

Sanjay Great point. People are looking at their first cloud relationships, and I think we need to look and see what happens when they divorce my cloud provider. The next one is prettier and I want to move to them faster. Encryption can certainly be a very key precaution in that

Peter Back to the original question, I think a lot of SMBs know that. They've got intellectual property. What SMBs don't know is that intellectual property is under threat from cyber threats, and that's probably the biggest perception challenge. Sure, they have key people they trust with it in their organisations, but they just don't understand about the cyber threat itself.

Aviv We did these analyst reports on our customers, where even in small organisations, or specialist small organisations, they tend to let data slip a little bit easier. It's mostly about awareness. That's definitely amplified by the use of devices, mobile devices especially, and I've seen a situation where a key executive actually accidentally leaked sensitive information just because they forwarded an email from their iPhone, not realising that there were actually attachments connected.

The devices that we have today, actually make it easie5r for everybody to leak data.

A colleague in Canada recently used an iPhone application to book flights through his airline of choice. Luckily device on his network actually detected a data leakage when he was trying to book a flight.

It turned out that that particular iPhone application did not encrypt the data, and would have sent his private card details, passport number, everything you could imagine you would have when you're booking a flight, and this is really significant issue. How much do we know about how secure all those apps that we use are ---- especially the ones that you sign in with. How do we know if they're encrypted or not? We don't really know. As security experts it's hard for us to know let alone if you're not in security and you don't' understand how this magic actually happens.

End of Part 1

Part 1 of *CRN*'s security roundtable appeared in the August issue of the magazine. Here is the second half of the discussion.

CRN Interesting you make a point about the operation of illegal cyber activity in the US perhaps attributable to their greater connectivity. Do you anticipate that Australia is going to be a very different security environment when the NBN comes on board?

Sean Certainly with our figures we saw a lot more systems compromised as broadband penetration improved in Australia. In the late 90s always-on-computing was not something that happened a lot, and it did provide a lot more resources for the bad guys to use as a compromised machine that may never ever switch off is quite handy, and this connection is always there. But I don't think that NBN itself is going to significantly change that because we've already got quite high penetration of always-on computers, and 3G and 4G networks mean that mobile devices are always connected. So the stage isn't really set for any kind of change, because that happened a while back.

Keith I think it will actually impact in terms of distributed denial of service. You hear quite often a DDOS is used to create some covering fodder. While you're busy in your data centre where the application is up over here, you have absolutely no idea of what is going on over there. So I do think that will rise because high bandwidth connected devices will be a great pivot point for a botnet to be part of a DDOS.

We saw 600 Gb in I what I think was the largest attack out there, which was a massive amount of data. It was in spam house I believe in Europe when they attacked them. We find that the Eastern European criminals use DDOS attacks as a diversion, and in fact the US FBI put out an alert for that specific thing.

CRN They're financially motived DDOS attacks?

Keith Yes, that's right and they will attack a site knowing that the IT people will be distracted through the malware we've talked about – come in through that remote access malware to move around.

Sean Yes, the ability to knock a site off the net, so that you can actually put up your DNS and DDOS is used as a tactical advantage.

Keith The flanking move is where they attack your website but come in through the back door to the financial system. The second one we see is like anonymous that are attacking by using DDOS attacks to make a statement and being very vocal about it.

Sean The other ones I've seen with DDOS things is gambling operations are particularly vulnerable and a thing has a very short lifespan and there's the threat say that 'we will take you off the net and you can't receive communication unless you pay us, because we'll take you off this event.

Peter Melbourne Cup day is a perfect example. Or you want to talk about Optus and Telstra and their partners coming together to have to do some filtering for that day, because it's amazing to do that, and maybe they pay them off and say 'hey please don't attack us'.

The NBN will allow different business models, and I think also we'll see the threats change because of those different models as well, so cars being online and everything will have an IP address. Those sort of different business models may change what and how the attacks, or what information the attacks can get from it.

Sean I see IPV6 adoption probably being a bigger problem in that space, because reputation filtering becomes much much harder, and that's when everything has an IP address, and that's when you have gazillions of IP addresses, and end-to-end connectivity for every device, so the idea of NAT (network address translation) goes out the window, firewalls become much more important. But I don't think the larger volume is going to be as much of a problem as the increased address space, for how do you defend against the attackers that come from umpteen million area.

CRN How important do you think educating end users about user behaviour, because we talked a lot about the need for organisations to have proper policies in place and to inform their staff about bringing in USB devices etc, but I've never worked anywhere where anybody has told me anything that I couldn't do.

Neil That's very interesting and on that point yes education is key. I find going to my clients, number one is that we've all touched on where the data is, 'What's important to you?' But looking at the SMB, what is the owner or the manager of that company's viewpoint on the information? Where does it go? The problem is that a lot of the time responsibility is handed to the IT department for example, rather than the management saying 'this is what you should do, and in the event of you not doing this X is going to happen' and enforcing that, as more of an HR approach.

Sean On that would you say that IT are given responsibility but not authority.

Neil That's a good point Sean. They are given both if that makes sense. The management will say 'it's an application what have you, you're in charge of that, but then fundamentally you are in charge of devices, and you should be in charge of all the facets that go with it'. That's where the danger starts.

Sean Yes, because what I've seen in quite a few organisations is IT guys being aware of a threat, but having no input to the business model. The separation between business roles and IT has been a big problem with 'we want to enforce this, but we can't because no-one has given us authority to do it'.

Aviv I absolutely second that. I've seen first hand and had multiple conversations with multiple security managers in Australia that they are absolutely sure that there is no shadow of a doubt that their data is being attacked, data is being leaked. But when I asked 'why aren't you doing anything about it?', they didn't have the authority. They had to prove it to an executive of sorts, and so it was a bit of a chicken and egg problem. How do you prove it without getting the authority, or budgets to implement the bare minimum to actually start probing. A lot of organisations have chosen not to know. 'I'd rather not know than be responsible'. Going back to education and how we deal with it, in SMB or even large organisations, what I saw as not so effective as having education to use it as a one- time effort, where you do a massive education and then we go 'okay we're educated, we did our workshop' – and you have to continuously interact with the users. You can actually train users to behave in a smarter way and behave in a secure way by interacting with them a little bit more about the different applications they use or different products they use, interact with them more, and let them know what they're doing.

For example, we've all been trained by the phone companies so that if we pick up the phone and hear a single line, we know the phone is working, because I have a line, if I dial the number and I hear a few short bips I know the number is busy and I have to call again. It wasn't written anywhere, the phone companies have trained us all to understand it, and if I take that analogy and bring it to security, I think we can probably create products that interact with users a bit more and train them what to do. Don't plug in this USB because you don't know what it is, it's an unapproved USB. Don't send that document, because it contains sensitive information, or do you really want to do that? Rather than having just one workshop once a year and saying 'we've covered that'.

Sean I agree entirely. The idea that you cannot be cruel and say 'we have to block this', but just alert people can change the behaviour massively. If you can pop up for web browsing, plug in USBs for copying certain types of data to certain places, generate a warning saying that 'by the way did you know that what you're trying to do, is this kind of problem?' People will think 'well no, no, actually I didn't'. It's not insider threats, it's actually just accidents, but being able to do that continuously trains people.

Sanjay We also need to enhance what we're educating users about. So if you look at the targeted attacks hitting organisations today, the vast majority are coming from 'spear phishermen' fishermen' that's occurring, because people are posting too much information on Facebook and Linked In. So it doesn't matter how much we tell people 'stop picking up USBs in the parking lot and putting them in' . That still happens, which is shocking, but it does. Start saying 'stop telling people on Facebook that you're really excited about your trip to New York in two weeks' and stop telling people that you're a fan of underwater basket weaving, because those are the things that are getting the emails saying 'here's your hot hotel room deal for New York, and 'here's Flo who's also in the underwater weaving class in your community; wouldn't you like to connect with her'. That's the other side of the coin, and that seems completely lost when you talk about user awareness today.

CRN To bring NSA back in again, Keith I notice in your white paper you cited the organisation's Deborah Plunk remarking that often security really needs to be approached from the point of view that you can't really keep yourself totally safe. The really bad guys are going to get in, and you have to mitigate and reduce the damage.

Keith Yes, we have to operate under the assumption that your network is already compromised, and you cannot protect everything. So we now must identify what's really critical to the business, and I appreciate that that is a daunting task for some businesses to know how to do it.

In my research I touched on the cyber kill chain and how that overlays an existing zone model architecture that I've been a big proponent of for a long time, about how we have internal and external users and service presentation business logic storage. Nobody has direct access to the data. They must be mediated by some web server, some business logic server that then accesses the data on their behalf as a way to manage and control that. Because that's how the attacker is going to get to it, and each one of those is a point where we can actually stop the attack and it's not just getting the data, they have to then get it out along the same sort of paths – so that provides a way to overlay that. If our networks are compromised, you can't protect everything, so it really means you've got to identify and protect that small bit. Even in somewhere like 'air gap networks', for example. Your master key and your HSM (hardware security mode) that should be a device that's not connected to the network. That forces someone to physically go to it to do something, or other examples like that. It's a new way, and we have to think about the problem differently, and to the NSA's point, they operate under the assumption they are compromised and then say 'what do we do?' on a daily basis. Your 60 percent or 80 percent of organisations that have malware in there, how do we go about our daily business knowing that and we wouldn't be able to define them, even with root kits and things like that, you might not always be able to identify where you're compromised.

CRN Can you give us a specific example of how the cyber kill chain might work for a typical organisation. What about a retail organisation, for instance?

Keith Okay so they are doing credit card processing. We talked a little bit about phishing and that's where they do the initial analysis and targeting. Then they have to get in, typically using some malware that some legitimate user clicked on and activated from a legitimate website, but with cross-eyed scripting and eye frames and all these other vulnerabilities. It has its place in the world for those things that get infected, and then that attacker can then essentially go out the front door, use an HTTPS like you would go to your bank or something. If I was an attacker, I'd put banks somewhere in my control domain so it would slip through a lot of that, and then that's how they establish a foothold, maintain persistence, go through to privilege escalation, identify the assets, exfiltrate the assets and then maintain the presence.

What the cyber kill chain is about is interfering with each one of those spaces. You have an opportunity to stop the attack, forcing the attacker to go back again. So if they're already in the network, how do we stop them from going from our work station in the corporate network to the data. Again we go through a business logic. We go through a secure storage and some database server that breaks connections with firewalls, RPSs, access control and all those controls, and each one of those point to get around is a kill point on the attacker.

Sean I agree entirely. The chains are fragile and if you can break any one of those points, there's generally no robustness and no work around, if you break that, you've stopped it.

Keith In an open flat network, once you're there you can move laterally anywhere you want to, and essentially own the whole network. But as soon as you start segmenting that with security controls, we just increase the complexity of an attacker to move around. Think about it like an onion with concentric layers. To get to the middle, you've got to peel each layer of the onion down to get to that information in the middle, and that's really how we should be looking at networks, and building and designing networks.

Peter One of the issues is this mentality of security professional that he's got to protect everything, and actually this is a perception of protecting everything, not just protecting the green zone, and it's really that bit, the education of the security front is teaching people that yes some malware, some lack of security is acceptable.

CRN A point you made in your white paper as well Keith is the increased complexity of vulnerabilities. If you read all the headlines in the technology media, you would get the impression that the number of vulnerabilities is increasing exponentially. Well yes it is, but as you point out the complexity of those vulnerabilities means that you don't have to worry necessarily about all of them, but you have to understand which ones you have to worry about.

Keith That goes back to the initial step of how we have to know the attacker, we have to know who they are, what their capability is and what their motivation is, how they're going to attack you and what they're after. That's all the threat scenario, and once we do that for each, and I've come up with eleven sorts of attack threat actors in mind, with nation state, radical active, like Anonymous, and even disgruntled employee and other sorts. You have to know each one of those, because they may be highly motivated but have low capability like a college student right? But if a nation state wants to go after you, like the NSA you're not going to stop them. If Anonymous wants you, you're probably not going to be able to stop them, and again it's a different way of looking at the environment that we're in, and we now know because we've taken Stuxnet and other ones, that was probably written by government agencies, and we've taken it apart and other malware we've reverse engineered it. That's proper software development that has gone through a rigorous quality process. Who can do that? Nation states that can have armies developing this software to attack particular people.

Sean I will also go with the bazar versus the cathedral for that. There are a lot of toolkits out now to create systems, and exploit kits which were saleable for licenses by culprits. But then that was leaked. They had this pirated, and it's $15,000 for a licence and then they released B2 and it has got better capabilities. So the software development thing is also quite broad and there is often outsourced components of it.

Patches on websites are just farmed out to huge armies of people in Bangladesh and so forth.

The market is there to outsource all of this. So what people find is that there is an actor that is hiring and the talent could know that they're writing Malware, or they could be like farmed out into operational components, and may not actually be a cyber-criminal as such.

Neil We're talking a lot about various different technology and all that, but I'm finding when I walk into organisations because they have purchased X Y Z technology, at a cost of X, they feel that they're in a nice secure place. Fundamentally what I ask organisations is 'Are you aware of your assets?' Not just your systems – it's the information that sits on them. It's the people that access them, and having a controlled environment within that space, and then from there, understanding the risks of that environment. From there you can feed in the technology that is going to mitigate that risk at that stage. Then I find that a lot of organisations tend to go 'oh I must have X' and run off and spend their entire budget on something that is fantastic in its entirety, but not necessarily in that environment.

Sean And this Neil has been happening for decades outside of security as well. If you've got a sales problem implement some system and then you realise we don't actually have a sales methodology. So this is not only a security issue.

Neil One of the usual assets that we always use is brand. We always talk to clients about brand, and I think Keith while I agree that a lot of those threat actors you were talking about, most SMBs would say 'you don't have to worry about those'. 'I don't need to worry about anonymous or hacktivist, because I'm a printing house that prints paper documents, or scan paper documents'.

Sean We've seen a very large security company be breached as a pivot point in order to get schematics and design from Lockheed Martin so why wouldn't an SMB or mid-market client also be pivot point and therefore they might lose one of their big flagship clients. It's important, but it's very difficult to quantify brand damage or brand as an asset.

Keith Reading reports like the Horizon Data Breach report we see that exactly. That's great because it includes the Australian Federal Police, the US Secret Service, the UK, NZ and Dutch I believe actual investigations and they show a lot of what they had and how they were compromised. They've all got bank accounts, and if the security is lame and you can hack their system to go in and move money out, even if it's thirty grand or sixty grand, not bad for a day's work, and we've seen that happen with municipal councils, and things like that where they can go in.

As we said before, they hack an attorney, because the attorney has a VPN to one of the mining companies, and the nation state wants to know about that mining company, before they go to a billion dollar spot price with a tonne of ore or whatever it might be and we know that those are real scenarios that happen.

I don't think there's anybody safe anymore. Depending on the hackers, and there's also a scale of hackers, that would be operating at a very low level, $30,000 is a lot of money. Others operate at a much larger level.

Sean It's also the ransomware market. It doesn't have to be hundreds of thousands of dollars, and that's a fast growing trend sector.

CRN There's some school in Queensland that got ransomware attacked and it cost them eight thousand dollars. For all we know that could have been a six year old child or something.

Sean This is the outbreak from outside, warning you have some threat to deal with, 'please pay us some money and we'll fix it for you'. Ransom ware has now become that. It's far more direct, and it says 'screw you, give us some money'. There's some few Windows scammers who try to convince you you're under threat from some legal entity, and Western Union is the way we always pay fines in Australia. But the ransom ware I agree with Craig has become very much the warhead of choice for targeting individuals, and small organisations, because these are really vulnerable because they don't block everything, they don't encrypt, so it doesn't take a long time. It takes Word Files, take Excel Files, take images, take the common things that most people will be using and hold them ransom.

Aviv I find it quite amazing. I recall reading research a couple of years ago from HB Garry that became famous or infamous in their own right for a different reason. They've actually published research that they claimed the organised crime is making more money today from computer fraud than actually from drug trafficking. So that will give you an idea that when it's financially motivated, where it's all coming from.

We know it's definitely an entire economy full of bad guys. There are 'bot herders' that sell bots to other attackers, be it spammers or spam for an organisation, organised crime or legitimate whatever it is that has other motivation behind it. They will sell services, you can buy some services online and there are tools online (with support contracts). It is generally things like a three month contract, but if our malware is detected, we'll give you some new ones.

Sanjay We talk about the bad guys a lot, but if you look at the people buying Malware, sometimes they're people we consider to be good guys, like large governments, who are actually just trying to attack other governments. So if you track some of the major attacks and go back to the people who bought malware, and you might be shocked who those purchasers were.

The other interesting thing is that we all know that we need more user awareness training, and we need to classify our data, but the opportunity to do that correctly may have closed. So five or ten years ago, the security officer might go to the CIO and say 'you know what, we need to take a six month hiatus here, from pushing more aggressively and let's get our security controls under control'. If you try to take that type of hiatus now, all your apps are going to be in Amazon the next day, because shadow IT is massive. So those windows are closing very rapidly and there's no opportunity to do it in any comprehensive way, you have to do everything at the speed of business now and that speed is very, very fast.

CRN With this ransomware, does anybody understand why there was such a spate of attacks in Queensland recently.

Sean I suspect some of that goes down to the fact just that it was reported. Qld Police has done a great job in involving the community and actually trying to raise general awareness. Qld police have gone further to try to create an environment where people are aware of the threats which are facing them. It may also be that there are a lot more people retired in Qld who aren't terribly secure.

Keith A lot of people retired to Florida and had the same kind of issue. It's a target for scammers because the people who are not technically sophisticated, have some money because they've retired, and at leisure mostly – but I think it's mostly down to reporting.

Sanjay I think it was eight years of State of Origin losses.

Keith I get calls every once in a while from someone who tells me that my computer is having malware, and I said 'oh really, okay' and they run you through to look at things and it's like 'let's make sure it's my computer, what's my IP address' and then they start swearing at me and hang up.

Sean My usual response to those is 'which one?'

Keith I say just to make sure it's me what is my IP address? That's still going on, and again the ransomware and scareware and stuff it's still happening. I got called a couple of weeks ago, and now I get tired, because I get called a lot. I said 'look just take me off your list, because I know what you're about, and if you're not going to give me my IP address, save yourself a long distance call and take me off your list, and call somebody else'.

Sean We started with this discussion saying 'all of this is not new, security is not new' and we all know that security is a process, there is no end of it.

Keith A journey not a destination.

Sean How often do we hear things like 'here's all the threats' and our conclusion is 'where'?

Keith We've got to think differently about the problem. Looking at some of the US companies that had Chinese attacks on them, that's where they came up with this cyber kill chain, again as a new way of looking at it. Then when I thought about it, it was like we need to understand the threat actors, what they're after and how they're going to go about it; how can we stop the particular one and there may be different kill points for different threat actors depending on who they are.

We know that we're compromised, and so we have a compromised network and really it's about thinking differently about how do we do this problem, because it has to be different thinking. You're right, all this stuff, it's been there done that, same thing. It's got to have a different way of looking at the problem, and this is how I ended up. I didn't plan to do that. Even though it's security architecture that's not new, stopping an attacker getting in isn't new; having flat networks, being evil isn't new. But now we can start putting it together maybe to learn from those things, and that's where I was really happy with the outcome of this, and it's actually got me thinking differently and now I can go back to my clients and say 'let's look at the problem from a different angle shall we, let's approach it in a different way' and you're right, we've all got these security widgets in there and we've got people which are our weakest link, but also our last line of defence. We've got all the knowledge that we have from everybody's good work and research here, but let's start thinking about it differently. So what are you guys thinking differently about as well?

Aaron I guess to simplify security is quite complex. You said before that it seems complex and it is and it can be, because there are a lot of ports, a lot of protocols a lot of products, a lot of different users. But if I could just simplify it down to users, data and the team we need the concentric circles with regard to the perimeter. We've come up with the latest go-to-market which is buy-in-protection. So ou need to think about the source of the threat, and if the threat is coming from the internet, then you may not be as concerned about the next generation capability to link that with active directory, because they're not in the active directory. You certainly will be worried about potentially the volume of traffic for the number of sessions, or looking deeper into the protocol to get some actual application protection. If the source and threat is internal, i.e. the victim of the spearfishing attack, then you probably do care about the next generation capabilities. Maybe an IPS or a botnet detector to look for outbound CNC. You certainly want to be able to correlate it then back to LDAP or Active Directory or some sort of user source.

Keith As an attacker I'd go after Active Directory as my first internal thing.

Aaron So then on to users, number four of the DSD (defence signals directorate) top four is privileged user management. So you have something that's watching the watchers. If you don't trust your DBAs (database administrators) and don't give them access to everything or do it unfettered or unwatched and unmonitored, you're going one step further to protecting that as well.

Sean I'd agree with that. Police privilege computing has not got enough credibility and Windows used to make it hard. Windows doesn't make it hard now.

Keith So should there ever be a domain wide administrator? That's a really good question. Why does one guy have access to everything?

Sean Certainly in amongst the deployments that we do for massive encryption and PKI it's all about separating out administrators from security officers. And even for certain circumstances having four eyes, like having a second person to authorise certain actions. Because if you don't have the privilege to pillage everything, then you can't pillage everything. Having said that, with modern malware there's a lot of stuff that doesn't rely on admin privileges. That privilege escalation is nice, but with a user computer you can actually spearfish within the organisation equally.

Keith My user ID is opposed to that, because eventually they will find out where I try to get onto a system if they're going to be successful. If they steal mine, they can logon and once they're in there, then they can go in there and do different things.

Sean Also the element of how many people stay logged in forever to Facebook, Twitter, Linked In, then whatever and 'remember my credentials becoming the default. So if you've got that user account, then you can be that user. Every time I talk about mobile phones, the question of 'do you lock your phone?' and people go 'no it's a pain' and so I say 'do you ever log out of Facebook?' No? Then when I steal your phone I will be you.

Aaron The third part about the puzzle I was talking about is data. So you need BYOD? You've got to look at it in terms of structured and unstructured data. Structured data is a database, and there are certain products which are designed to look at the databases, look at the privileged users, look at the SQL protocol, moving in and out of it and what's happening or the queries you're doing. Is there a massive select statement that's actually trading a whole lot of data that isn't normal?

The other side of it is actually security which follows the document. Everyone is probably familiar with Microsoft DRM. It's a pain to link; to federate your trust with your domain and another. There are now independent products that actually bind controls to the document and then it doesn't really matter where it goes, you can have a central console that can see where it goes and what device it's on and which user printed it, copied it, and you can restrict those sorts of controls.

Peter Moving on with Keith's comments as well, I also think there will be a trend to move from individual security, to more collective type security – so there's going to be a lot more information sharing, and a lot more working effectively, not just with security services, but even governments sharing much more information together. A security social network.

Sanjay Back to SMBs, if a small business can't have this type of conversation with their channel partner, the reseller partner, the trusted security adviser, they probably either want to encourage it or augment it, because these are the issues of today.

Multi page

Follow us on Facebook and Twitter

Email this | Print this | Tweet this | Send us your tips | SHARE

You must be a registered member of CRN to post a comment.

Click here to login | Click here to register

Top Stories

Melbourne IT nabs Optus broadband boss as new CEO

Mercer takes over from Hnarakis.

Technetics clinches major Apple account

Punt on public tender pays off.

Melbourne iPhone app house is new AWS cloud partner

Channel evolution in full swing as