

## The Importance of Being “Security-Minded”

By Stephen A. Braithwaite, CISSP

[email: [blog@nitefall.co.uk](mailto:blog@nitefall.co.uk)]

At InfoSec '07 Bruce Schneier gave a talk on “Do We Really Need a Security Industry?”<sup>1</sup> It's understandable the perspective he's coming from – his inclusive single-source one-stop-shop is something that Counterpane, his company can produce now they are part of BT. Bruce has also put forward to the House of Lords in the UK; that legal liability needs to be shifted towards the manufacturers and suppliers of hardware and software<sup>2</sup> - though to be honest, the term “systems” would be broader description capturing all potential failures.

I've been mulling over this for some time, and my initial thoughts were: “Of course!”; “Makes sound economic sense”; “Rationalisation of the security industry into Systems Providers would be great!”

Then I fell out with the idea. There are several reasons why I think this is, and more you could probably come up with yourself. But the basic gist is this: “security is not a product – it's a process”. It's a famous quotation that any Security Practitioner would recognise – it was coined by Bruce himself. By out-sourcing your infrastructure provision – which includes security protecting your data; you're in effect “buying the security product”. This is where it gets tricky. Yes, you are out-sourcing to a third-party supplier who by rights, must be following the mantra of implementing security processes. But it's a product none-the-less. It could well be the same product that your prime competitor is buying, identical in every way but in faces who turn up to implement it. The configuration would be the same, the same hardware, the same firmware, the same software, the same applications, the same release-versions; the list just goes on....

There's the flaw: It's all the same.

Humans are by nature, lazy. You can argue that point forever, but by and large what is good enough to be created once, then it'll be re-used again. And again. And again. Until in fact, it is deemed flawed or redundant and needs to be upgraded or replaced. Now, what happens if we all do move to single-source providers of our information systems? Well, corporations will have a single source of complaint when something in their information systems infrastructure goes wrong; they have one bill to pay; and they have one single resource to have to control. In the grand scheme of things, it's a winner for service providers and companies alike. But I fear that amalgamation.

In industries all around, since forever perhaps, there has been vast consolidation. As the most obvious example in the UK right now, look at the Broadband Providers. At the start of the “broadband revolution” there were a multitude of providers, really huge numbers of providers and sub-providers, perhaps as many as a hundred. All different to some extent, with competitive advantages to be gained by the customer: the end-user. Some had great service, with top-notch hardware and bags of capacity. Some had help-desks where you could reach someone 24/7. Some had signature-based filtering on their routers which would stop malware from reaching the broadband endpoint in your house – to some extent.

Now, in essence, there are pretty much three providers: Sky, Virgin Media, and BT (with Orange, Carphone-Warehouse, and Tiscali trying to hold their own). Some still haven't gotten around to de-listing their old names, such as Nildram to Pipex, Pipex to Tiscali - so users of say, Nildram, don't probably know they are actually provided by Tiscali now. As long as it works, end-users don't care.

The providers have done this because they can see the market: They see that THIS is the way that they can control huge revenues by delivering content to people. It's the only way of delivering true on-demand media in whichever form: Video/Voice Communication, On-Demand Subscription/Global TV, and something called, The Internet. At some point, these providers will be the prime lucrative form of generating and controlling the vast majority of advertising revenue – which they will demand charges for. So, to capture as many people as possible, they buy their competitors. And guess what, one of them even bought out their end-user hardware provider also, so now they can mass-produce a single machine that will go into people's homes - a third of people's homes. This machine must be connected to the internet, or at least, the providers' network which is connected to the internet – which amounts to the same thing. Now a third of the population running one identical internet device, on one identical network; has to be cause for concern. Again, this machine will have the same hardware, firmware, software, configuration, etc. as all the rest. And that's the flaw. It imparts a single point of failure to one-third of the UK's home internet users. It's a massive target for criminals and malware perpetrators who will begin almost immediately to try to exploit this single huge target. They will. And at some point, they will succeed. So why hasn't that happened in the past? The simple answer is complexity.

The Broadband Box that will be delivered to one-third of end-users at home will have huge amounts of code, a complex operating system, and custom applications. It will need to, because it'll have clever jobs to do.

Unsure? Take a look at a common or garden Netgear ADSL+WiFi you can buy now. Now go look at their support website for that product. See anything interesting from a Security Practitioner's perspective? Yep – updates. Lot's of them. There are patches, and many of them for security reasons. Ever applied any? Did you know they were even there?

Have you experienced a data-leakage resulting from running an older firmware on one of these boxes? Who knows? I've said before, manufacturers of these sophisticated embedded devices should have their own equivalent of "Patch Tuesday", and include some obvious method of updating users: A mandatory email, a Pop-Up sent from the embedded-device, heck – even flashing Red LED on the front of the device would be better than nothing (though could be tricky to see if you keep the box tidied away in a cabinet).

You can't predict what is going to happen in the future – you can make educated guesses, but it's mathematically impossible to model potential flaws that may occur in your systems down to the nth level. That's why so much security is retrospective – it's about learning for the next time, adding that to your current security model, and putting better systems in place by identifying weakness, and reducing risk.

Now imagine your current PC/Server setup. Most likely it's running Microsoft Windows – whatever flavour. Yep, you will have some other stuff in your business: A few Mac's in the Art Department; a few Linux Servers; some Linux, SunOS, or WinXPe Thin Clients; some Linux or VxWorks embedded on your WiFi Access Points; Cisco IOS on your network devices; Google Linux on your internal Search Engine; even some goofy HP OS that runs the Server software in your Networked LaserJet Printer. [I hope you have these on your Patch-List, by the way].

Back to that PC/Server: By far and away, the vast majority of malware will be targeted at those Windows systems – and you have stacks of them. They're the core function of your information systems. Even if they are not, whatever else you're using in similar numbers presents the same risk.

Now those Windows systems aren't targeted by hackers and malware perpetrators for nothing: The latest Trojanised-Worm isn't built by specialist criminal hackers because they don't like the name "Bill", or think that the Microsoft logo is dated. No, they do it because that's where the money is – that's the way they can hack in. This is not because Microsoft's products are the most insecure – nowadays nobody argues that they are pretty secure. It's because of one single flaw: It's all the same. Out-of-the-box default security is what is commonly used by many individuals and companies. Even those within governments or healthcare are relatively "raw" and differ little from what came shipped on the PC/Server. Do you think someone would harden the printer configuration, change default settings in the router's table for access, and fiddle with the SQL server's defaults? Unlikely. It's the same generic platform's that are the choice of the successful hacker. The same Services enabled in the Windows client system that allow an extra dimension to be added to their attack-surface. The same reason why Microsoft's IIS used to be the laughing stock of web-security: Because the defaults were awfully insecure.

By having a single large target we create an opportunity for hackers to concentrate a lot of resource on a single point of failure – even if it doesn't exist right now, they have the objective in mind to find a flaw and exploit it. That's the issue.

Our differentiation protects us to a great extent from the really bad worms that existed in the early 2000's. Slammer, et. al. most probably couldn't exist in the way we have information systems now. Yes there are flaws discovered in Microsoft products nearly every month. Yes there are flaws discovered in Linux, Cisco IOS, and all the other things we run. But there have not been any massive failures, unlike in the past – and a lot of that is solely to do with incredible growth of the Security Industry and the independence of Security Practitioners, yet professionalism they exert. What one group of practitioners see as a failure, others see as an opportunity to learn and guard against. Whilst it's true - closing the stable door after the horse has bolted is a waste of time: It's only a waste of time for that one horse. Besides, next time you might not only see that the stable door must be shut, but also that it must be over two feet tall to stop the horse leaping over it if it chooses. It's a process. It's a learning process. It's retrospective – yet pro-active. This is what being a Security Practitioner is all about – it's a more significant fundamental than ensuring the boxes are all ticked, it's about being Security-Minded.

Being Security-Minded is essential for being a CISSP. If you weren't, I guarantee you'll find it nearly impossible to pass the CISSP exam, because the questions posed are not simply "tick-box questions". They're, dare I say it: "Out of The Box" questions. They are challenging not just your knowledge – not just your understanding, but your imagination, your cunning, and your awareness. This is what being Security-Minded all is about, and this is what Bruce himself says he looks for when employing someone. If you are Security-Minded, you will see that the lack of differentiation will cripple a significant sector if the homogenous security-product is provided by just a few Service Providers. You'll know straight away, that there will be significant configurations that are alike, even down to default passwords. This is the norm. This is what happens when companies merge and their IT departments are amalgamated. If it happens between a couple of companies merging their IT departments, it most certainly will happen when there is a cost-benefit ratio to be gained by forming "strategic-alliances" with chosen suppliers. Which of course, basically means someone supplying a security product to you, will give you a bigger discount in terms of a greater number of boxes shifted – and you only need to learn one product.

This amalgamation is bad for security, and absolutely critical for the Security Industry. Don't go down this route, don't homogenise, don't become box-shifters and box-tickers. Let's keep our independence and our professionalism; our different ideas and ways of doing things. I sincerely hope that companies will seek professional advice, and out-source any provisions they need in respect to setting-up and implementing their systems. But get your security from someone who isn't tied to the same people who put a PC on your users' desks, servers in their racks, and giving firewalls passwords. Get someone who'll look at it independently and some who's going to be Security-Minded throughout. Or better yet – build your own people who'll have a vested interest. After all, it's their job the business succeeds.

<sup>1</sup> [http://www.schneier.com/blog/archives/2007/05/do\\_we\\_really\\_ne.html](http://www.schneier.com/blog/archives/2007/05/do_we_really_ne.html)

<sup>2</sup> [http://www.schneier.com/blog/archives/2007/08/house\\_of\\_lords.html](http://www.schneier.com/blog/archives/2007/08/house_of_lords.html)