

## Leveraging compliancy standards for a better network

I first approached this idea in January of 2008 when I started to recommend to eSubnet clients that they should consider PCI as a source for best practices. I am grateful to have this opportunity to share my ideas with all of you today.

Specifically, I'll be going through 6 key tips on configuring and managing your network and your security.

First let's begin with organizations which offer these standards. There are generally two types.

### **The voluntary standards**

Included here are organizations such as International Organization for Standardization (ISO), System Administration, Networking, and Security Institute (SANS), National Institute of Standards & Technology (US) (NIST), Center for Internet Security (CIS), Information Technology Infrastructure Library (ITIL), Control Objectives for Information and Related Technology (COBIT), and many more. These organizations offer guidelines and requirements covering managing processes, writing policies or configuring devices in your environment often followed by an audit process.

### **Carrot and Stick**

Then we have the so-called carrot and stick certifications. Here we find legislated and regulated requirements as well as voluntary standards such as Payment Card Industry-Data Security Standard (PCI-DSS). I call them "carrot and stick" certifications because these ones use both rewards and penalty incentives, typically financial in nature.

And while PCI is a voluntary standard, the stick applies if you don't adopt it. You pay a credit card transacting premium for non-compliance.

All of these standards are created in cooperative environments and via collaborative processes. This means that the backing organization put together some pretty smart minds in order to develop and deploy the standard. I look at these efforts as think-tank equivalents.

Take advantage of these peoples' efforts and hours. The standards can guide you towards a better and more secure network environment without you having to spend your precious time and energy coming up with ideas. The wheel has been invented, why invent it again?

## PCI-DSS

The PCI-DSS is currently at version 1.2. Version 1.1 was made obsolete December 31, 2008. It began though with what I consider to be one of the best compliancy questions.

“Does your firewall configuration match your security policy?”

This question elegantly covers four areas of concern in security management:

1. Is there a security policy in place?
2. Are the people configuring the firewall aware of the security policy?
3. Is the firewall configured against this policy?
4. Is there someone looking at the firewall configuration work to insure it remains within the standards of the security policy?

With version 1.2 the question I quoted was lost. The spirit of the question remains as you will see.

At eSubnet, we developed a process for using these various standards to supply you with a health check.

Our NET-SEC Tool helps explore whether you've adopted best practices for networking and security. The version of the NST discussed today is based on the PCI standard and future versions will show alignment with other standards.

I selected PCI due to its current popularity and the carrot/stick nature of its financial penalty. And please note, even if you don't accept credit cards you can use PCI to evaluate your network and security.

Using the NET-SEC Tool, we cover various aspects of your practices. I'll briefly review 5 of the questions today. You can follow along by looking at the print copy of the NST provided.

1. Section 1.1.1 of the PCI-DSS looks at Change Management and service availability post change for routers and firewalls.
  - o Services availability is why the network was built. Every year more business processes are moved to the network.
  - o Having a checklist of the services supporting these processes and testing against this list is the only way to ensure that end-users internal and external will have the access they need
2. Section 2.1.4 asks if the security policy provides business justification for all protocols and ports permitted by the firewall.
  - o What resources end-users both internal and external have access to is an important part of securing the network.
  - o ICT staff and consultants are well positioned to implement security requirements, but setting the requirements should be left to management. Management has the business knowledge to properly evaluate risk. This sort of business justification can be applied to more than just protocols.

3. Section 10.4 raises the question of clock synchronization.
  - o If you do keep logs of critical events for your network devices then having their clock synchronized makes my job easier when you call me in for a post incident review.
  - o What I am talking about here is Network Time Protocol (NTP).
4. Section 11.4 of the PCI-DSS focuses on network scanning, both internal and external.
  - o There are a number of vulnerability scanners or test tools available online.
  - o And, while we all make every effort to stay on top of patches and updates invariably something is missed.
  - o To be blunt – The bad guys scan your network and will leverage vulnerabilities when they find them.
  - o When having your own network scanned I recommend that you have someone other than the network security team perform the scans.
5. Section 12.9 asks about a data spill plan.
  - o Everyone understands the importance of a business continuity plan to insure productivity. A data spill is a different kind of disaster.
  - o Legal offices are especially sensitive to this sort of incident due to the solicitor-client privilege on information.
  - o Additionally, notification of data breaches is being legislated around the globe. The Canadian government will most likely follow suit.

Now for 1 question I included in the NET-SEC tool outside of PCI

6. NST question 1.1.9 asks about historical data for network traffic.
  - o How many times has this happened to you? Walking down the hallway you pass someone who complained about the network being slow early that day or even the day before.
  - o You have little to no hope in explaining the situation or even beginning to know where to look as this all happened in the past.
  - o By retaining historical data you have a starting point. Something as simple as MRTG (The Multi Router Traffic Grapher) you can at least see if the slowdown was network wide or an isolated incident.
  - o Additionally you have solid numbers for capacity planning towards the future. Not just end user opinion.

To sum up, by following the intention of a standard even if you don't need to follow it to the letter, you can improve your network, your security and therefore the availability and integrity of your data.

The more you are able to stay on top of your network performance the less likely there will be outages or other problems. Without problems plaguing them, your users can work productively. Being proactive in ICT is a win-win for everyone. Leave the reactive responses for the true emergencies.

To find out how proactive you are, please go through the copy of eSubnet's NET-SEC Tool. To request the eSubnet NET-SEC Tool visit <http://www.esubnet.net/net-sec-tool.html>

One last point for you, if your firm does take credit cards, how that information is managed, stored, and secured should be of concern to you.

Thank you

## About eSubnet

eSubnet focuses on solutions that set industry-leading standards in these areas. We offer customized network solutions for large business and enterprise clients. We work with our customers to develop intelligent solutions that fit the technology to your business, not the other way around. eSubnet will help you to maximize the potential of your business.

eSubnet is based in downtown Toronto. Our location in the center of Canada's financial infrastructure allows us to respond rapidly to critical emergencies. We stand ready to ensure the integrity of your network services--whether your business is on the same block, or across the country.

## About our Founder

Richard Danielli, President

Richard Danielli is the founder and president of eSubnet Enterprises. He has broad expertise in the fields of networking and data security. His numerous industry certifications include Cisco Certified Network Associate (CCNA), Cisco Certified Design Associate (CCDA), and HP OpenView Qualified Professional.

Mr. Danielli has been a key contributor to multinational projects in both North and South America. Under his leadership, eSubnet's client roster has expanded to include some of the major names in Toronto's finance, art, legal, and medical sectors.



Mr. Danielli currently resides in downtown Toronto, in close proximity to eSubnet's offices and the clients he serves.