



I need  
complete network security  
that's affordable....  
and  
I needed it yesterday.

## **Disposable Security Technology**

**Kevin Prince**

**Chief Security Officer**

**Perimeter eSecurity**

**April 2007**



*Complete. On Demand. Affordable.*

## Disposable Security Technology

I remember learning (and being disgusted at the same time) that the New York Landfill, located on Staten Island was one of the two man-made objects that can be seen from outer space (the other being the Great Wall of China). This New York Landfill accepted over 2 billion tons of trash during its 50 year existence. The landfill is over 2200 acres in size, compared to the 13 acre base of The Great Pyramid of Giza

This disturbing fact came racing to mind when I kept seeing announcement after announcement regarding security technologies that were getting the status of “end-of-life”. With the number of security technologies more than tripling over the last 5 years (according to Gartner), each of which are designed to mitigate a specific security threat, I wonder how financial institutions (FIs) are able to keep up with it on all on their own. The quick answer is, “they can’t”, and more disturbing is that, “they don’t”.



Several years ago, it was quite common for a financial institution to hire an IT person where one of the duties of that employee was IT security. Since that time, that job has gone from part time, to full time, to having a team of IT security experts.

The employee cost is just one element. It used to be that a firewall was all the IT person had to worry about. Now with literally hundreds of different technologies each with their promise of reducing or eliminating IT security risks, most financial institutions have dozens of different risk mitigations solutions deployed, with many in the hopper, and more on the “wish list”. Each of these technologies going through an IT security lifecycle of Review, Purchase, Implementation, Management & Monitoring, and Upgrade quickly made it overwhelming for FIs to do on their on.



The answer for most FIs is outsourcing. This movement over the last couple of years has been tremendous. Even large FIs have seen the value in outsourcing. As a result of this movement, new

challenges need to be faced, namely selecting a provider for outsourcing, and prioritizing the security solutions you need to deploy.

### SELECTING A SECURITY PARTNER

With literally hundreds of managed security providers, what criteria should you use in selecting a partner? FIs need to realize that not all managed security providers are created equal. The very first thing you should look for in a managed security provider is whether they are held to the same level of government compliance that you are held to. So ask all existing and any new potential providers if they are under FFIEC oversight.

Most providers are not yet on the radar of the FFIEC, and therefore, often don't meet the standards necessary for true security best practices. This alone will cut your list of potential providers to a very short list. Next, ask them how many years the FFIEC has been visiting them. Be sure you select a provider that has a minimum of two years under their belt, and I would suggest three.

Next, be sure that your potential provider performs audit reviews to include, at a minimum, a SAS70 Type II audit and a third party security test such as a Cybertrust TruSecure testing and certification process. The results of all of these should be available to you for review and part of your required 3<sup>rd</sup> party due diligence for compliance.

Following that, you should select a vendor that provides and supports a variety of solutions. Most providers offer 3-6 products or services. With the ever growing number of solutions needed, this causes each FI to work with many vendors. This has exploded into a major problem around vendor/partner management. If you select a provider that has a large number of services, and does them well, it will reduce the number of partners you need to work with, and ultimately make you life a lot easier.

Lastly, select a provider that has an option for "in the cloud" services, otherwise known as "On Demand" services. This is where you would have all your Internet traffic piped through their systems. Through this process, you can leverage millions of dollars of infrastructure as well as a more dynamic updating to deal with new threats. Now it is your provider's responsibility to deal with the technology lifecycle, not yours. This is ultimately the solution to the technology landfill problem with devices having an ever shorter life span (now between 2-3 years on average). Not to mention, by using On Demand services, a provider usually has the capability to protect you better because they are seeing you and potentially thousands of other customers like you. With this aggregate of information, they can respond and protect the customer community much better.

## PRIORITIZING SECURITY SPENDING

All too often we see FIs spending money on the wrong security solutions. Unfortunately this is due to the reality that a majority of the FIs education on security issues comes from sales people...these same individuals that sell 3-6 products or services. So often, the right system(s) do not get purchased or deployed.

All FIs are required to do a complete IT risk analysis. If done properly, a FI should be able to identify weaknesses in their security posture and then evaluate the appropriate technologies to fill those gaps. A good risk analysis will prioritize business systems and processes, so you will want to apply additional security risk mitigation strategies in the areas of highest risk.

Some online tools are also available to assist with an IT risk analysis including Risk Profiler, a risk analysis tool developed by Perimeter eSecurity. This tool can be found at <https://www.riskprofile.org>.

## CONCLUSION

Teams have now been selected to submit project plans for the reclamation of the New York Landfill. Hopefully, one day, as we look down on the earth from space the sign of intelligent life will not be a landfill. Similarly, I hope that FIs can begin planning and aligning their needs with their security budgets and work with qualified partners to create an environment of maximum security for the FI network to ultimately protect their customer's sensitive information.