clavister ThoughtLeader

# Has PRISM Scattered Trust in IT Security

John Vestberg, CEO of Clavister looks at whether organizations can truly trust their security solutions to safeguard their data and intellectual property, post-PRISM.

In the IT security and comms markets, it's been difficult recently to escape exposure to what's known as 'lawful interception'. It's a concept familiar to many working within the security industry, and even to many members of the general public: normally, a court order is issued for surveillance, and it is then done with the cooperation of the ISP, telco or network operator. It's a well-documented, clearly traceable process with a legal basis and offers no surprises.

However, the uncovering of the NSA's PRISM surveillance project, which has allowed industrial-scale access to the data and voice traffic, stored information, file transfers and social networking activity of both individuals and organizations without their knowledge or permission, has provoked a mass outcry.

It's bad enough that cybercriminals have for years been illicitly accessing data and intellectual property, and using it to their own ends – but it's even worse to find that Government agencies may have been doing the same. And while Government officials rush to inform companies and the public that PRISM isn't being used on them, and there are safeguards to ensure that their data and records are not being compromised, this is doing little to reassure anyone.

## Undermining the 'trusted network'

Of course, there has been speculation for some time that the intelligence agencies of the superpowers have had the ability to unlawfully monitor individuals and gather information using in-depth knowledge of networking and security solutions and software. Now that this speculation seems to have been confirmed by the news about PRISM, it raises a critical question: can equipment and software originating from countries involved in such information-gathering really be completely trusted and relied on for corporate security?

Recent developments involving the multinationals that provide much of the networking equipment, comms applications and search engines that forms the infrastructure of the Internet and other global networks, indicate potential threats to privacy. Threats to individual privacy as well as enterprise intelligence and national security.

The fact is that the majority of all Internet searches use a single search engine, a substantial proportion of smart phones come from one vendor, and the majority of operating systems and cloud e-mail servers originate from just one source. Any of these organizations might be required to assist their domestic government with information gathering related to national security or perhaps for economic advantage.

## Trust me – and my 800,000 colleagues

This begs further questions. Can these suppliers be trusted with private information or sensitive intellectual property? Could confidential business intelligence and intellectual property be secretly taken and used for economic gain? This activity need not be supported by a government department: over 800,000 people in the US hold top security clearances. That's about the same as the population of the city of Stockholm. Can every single one of those 800,000+ people

be fully trusted? Remember, we now know about PRISM because of the actions of a single individual who had access to top-security material.

Cloud applications provided by Facebook, Google, Skype, Yahoo and others, are widely used by business to attract customers and to build relationships with them. Banks, for example, might interact with customers using applications on social networking sites. Even if the meeting doesn't involve exchanging confidential information, it could possibly open a route via the application into the server farm of the bank, to retrieve protected information.

Possible backdoors in networking equipment such as security gateways and firewalls must also be considered. If such backdoors exist they could give an external third party an untraceable way to interfere with traffic flow. One method of making use of a backdoor in networking equipment is known dynamic port knocking, which is undetectable and leaves no trace, but could give a third party total control, allowing them to eavesdrop on, or intercept internal traffic.

So with accusations and counter-accusations flying between the West and the East about who has been accessing what information, and to what end, and denials from the vendors named in PRISM, where does this leave organizations that have serious questions about the integrity and trustworthiness of their networking and security solutions?

I believe that organizations will start to evaluate their risk of exposure to government-sanctioned snooping. They will reconsider their usage of, and reliance upon, solutions from the established 'big names' from both the West and the East, and will start to evaluate alternatives that have not been tainted by this loss of trust. As the old saying puts it: trust is like a mirror; you can fix it if it's broken, but you'll still see the cracks.

## More From Clavister

For more though leader articles and information about Clavister products, visit **www.clavister.com**.



Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com