Reputation is everything: what does ‘trusted security partner’ really mean?

By Paul Jolliffe, DSM Expert: Security at T-Systems South Africa

- ‘Trusted partner’ is more than a tagline – it encompasses a broad range of aspects
- Your security partner should imbue principle of integrity, reliability and transparency into its DNA
- It should also be playing an active role in safeguarding our society from the risks of data theft and misuse

Information security is rapidly ascending to the top of boardroom agendas, as firms continue to digitise, and as more and more of their value is attributed to their data.

It’s true: data truly is the new currency of the information era.

In the same way that a company’s financial assets are protected by carefully selecting accounting, auditing, banking and investment partners, it’s data assets must be protected by choosing the right information security partners.

At stake are some of your most valuable assets – your data and your reputation.
Because of this, the reputation of your security partner is paramount. Almost every technology shop has latched onto the tagline of ‘trusted’ provider. And trust is, indeed, the name of the game. As an organisation, you need to implicitly trust that your security partner is accurately assessing your vulnerabilities, planning for future threats, implementing the right solutions, and quickly responding to any breaches that may occur.

But the term ‘trusted’ is far more than a marketing tagline. It should, in fact, encompass a broad range of attributes:

- **Accountability**… look closely at the contract to see who bears the risk burden? Your security partner should have the confidence to shift the risk away from you, to themselves as the service provider.

- **Technical skills, capabilities and certifications**… your partner should assemble multi-disciplinary security teams to cover every contour of your threat landscape, to provide the broadest breadth of services.

- **Continual innovation and consulting**… being a ‘trusted partner’ means proactively discussing issues unfolding on the threat horizon, providing consulting services to mitigate these threats, and continually innovating in one’s security approach.

- **Strong customer satisfaction levels**… security partners should participate in industry surveys, regularly measure feedback from clients, and use this feedback to refine their customers’ experiences.

- **Deep relationships**… does your security partner invest in developing a long-term strategic relationship, or are they merely seeking profit margin on security solutions?

- **Developing your company culture**… so that your people become more aware of security and risk management, and make more astute decisions - never revealing sensitive personal or company information.

- **Effective ways of contracting and pricing**… contracts should certainly not lock you in for years at a time, and pricing should be aligned to clearly-defined business performance and outcomes.
Selecting your security partner shouldn’t necessarily be about finding the most inexpensive, simplest IT firm or solutions. When it comes to something as critical as your data, it's wise to find a strategic partner that imbues principles like integrity, reliability and transparency into its very DNA. You'll need the confidence that your partner is acting with a high degree of ethics, and acting in your best interests, at every turn.

Value-added, truly ‘trusted’ professional security companies should be active in the spheres of public debate and policy-making – recognising that data security is likely to emerge as one of the biggest social issues of the 21st century.

While Big Data holds the promise of improving our lives at every level (think about the safety of self-driving cars or the increasing connectedness of terrorist activity surveillance), it needs to be carefully managed. As devices like the Amazon Echo start entering our homes, potentially recording everything we say, and Google Maps plots a history of our every movement, the notes of an Orwellian dystopia starting ringing eerily in our ears.

The onus is on security professionals to advise individuals, organisations, and governments on how to balance transparency and privacy, when to encrypt data, to anonymize data, to classify data.

It's certainly not too much to ask of your security provider to have an active voice and play an active role in the broader social issues relating to data privacy.

**T-Systems in South Africa:**
Communications Specialist
Thamsanqa Malinga
Thami.Malinga@t-systems.co.za
+27(11)2547400 (Phone)
About Deutsche Telekom
Deutsche Telekom is one of the world’s leading integrated telecommunications companies with around 151 million mobile customers, 30 million fixed-network lines and more than 17 million broadband lines (as of December 31, 2014). The Group provides fixed network, mobile communications, Internet and IPTV products and services for consumers and ICT solutions for business customers and corporate customers. Deutsche Telekom is present in more than 50 countries and has approximately 228,000 employees worldwide. The Group generated revenues of EUR 62.7 billion in the 2014 financial year – more than 60 percent of it outside Germany.

About T-Systems
Deutsche Telekom considers the European business customer segment a strategic growth area. Deutsche Telekom offers small, medium-sized and multinational companies ICT solutions for an increasingly complex digital world. In addition to services from the cloud, the range of services is centred around M2M and security solutions, complementary mobile communications and fixed network products, and solutions for virtual collaboration and IT platforms, all of which forms the basis for our customers’ digital business models. With approximately 47,800 employees worldwide, T-Systems generated revenue of around EUR 8.6 billion in the 2014 financial year.

Since the inception of T-Systems in South Africa in 1997, the company has cemented its position as one of the most successful T-Systems companies outside of Europe. A leading ICT outsourcing service provider locally, T-Systems offers end-to-end ICT solutions in both the ICT Operations and Systems Integration markets. Their extensive portfolio of services covers the vertical, horizontal, IT and TC space. T-Systems South Africa’s head office is located in Midrand with another major office in Cape Town, and 20 further representative offices in locations throughout southern Africa.