



Key to Survival

Be More Adaptive in a Converged World



Dwaine van Vuuren

Dwaine leads Dimension Data's global Security business. He has a strong track record of more than 15 years experience in IT security, corporate governance, risk management, security assessments, and managed security. Dwaine was also one of the Dimension Data visionaries who created our Global Services Operating Architecture (GSOA). This framework governs how we design, deliver, and support the services we provide to clients.

Modern enterprise architectures have become more complex over the years. The security practices to protect these infrastructures have often not kept pace. But it's not too late.

Convergence has changed the world of business. The increase in the use of PDAs connected to the network, laptops, outside consultants and wireless technology, creates multiple new entry points and increased risk. Compliance issues further complicate this scenario as governments are enforcing legislation demanding that organisations take responsibility for the protection of their data.

Dwaine van Vuuren, Global Practice Lead: Security Solutions at Dimension Data says, "Networks are becoming extremely complex and interconnected with third parties. Today, a large percentage of business devices support multiple networks, and PDAs and mobile phones are delivering e-mail and messaging, to name but a few examples. No component is of equal maturity in the value chain."

"When you work with different technologies and levels of maturity, security can become extremely complex."

He predicts that pervasive network security will impact everything in the next couple of years - from client software to the security devices on the network infrastructure in the backend. Organisations will start driving the purchase of integrated security products, and the emerging new category of Network Admission Control (NAC) is bound to grow in the next couple of years. A key consideration, according to van Vuuren, is to ensure that the technology decisions today fit with a long term security strategy.

Create an Adaptive Infrastructure

Van Vuuren speculates that to create an adaptive infrastructure, as a starting point, organisations will investigate the myriad of security vendors available in the marketplace to supply them with the technology.

Interoperability, investment protection and standards tracking are all key considerations when evaluating possible vendor-driven solutions. However, the success of the adaptive infrastructure within an organisation not only depends on specific vendor technologies, but also on a framework that encompasses a coherent security approach.

Van Vuuren says, “To cater for security of the next generation of communication infrastructures, it becomes essential to deploy a framework that transforms the way organisations administer access to their network resources. Dimension Data has worked with customers and vendors to develop such a framework, which we have branded the Adaptive Secure Infrastructure (ASI).”

The ASI framework aims to create the foundation for a dynamic, manageable and impenetrable security infrastructure within and around organisations – where the appropriate levels of trust and access granted to various users are clearly delineated, controlled and enforced. It takes organisations through a process that includes the following phases:

- ▲ Identification
- ▲ Classification
- ▲ Isolation
- ▲ Control

Van Vuuren elaborates that in the **identification phase** it is essential to analyse the existing environment to establish the number of users, systems or even applications connected to it. Such elements as computer, user role, health status, access method and location are part of the identification process and together they form the ‘entity’. This phase is critical to achieve control based on context and relationships, which is the end goal.

During the **classification phase**, the risk profile for each entity is identified. The classification process takes a series of factors into account, such as the protection mechanisms deployed at the entity and the value of the data that will be accessed.

In turn, during the **isolation phase**, the entities are separated into different groups, based on their risk profiles. Entities with similar profiles are not authorised to communicate with entities with a different profile. The same segregation is further utilised to separate entities with similar profiles to reduce the propagation of any threat and the implementation of end-to-end security.

Van Vuuren says the last phase focuses on **control**. The system is secured by implementing appropriate and specific security measures within the overall IT architecture. “For example, a mobile user would typically be allowed access through the VLAN, where a particular segment on the network would also be conducting an additional security check on the user.”



ASI Suitable for Anyone

Van Vuuren comments that the ASI framework is open and agile and suitable for any type of business – small to medium size or large enterprises. The framework fully supports the convergence in the IT infrastructure in terms of voice, video and data, the increased integration of security into operating systems and network infrastructures, and also has no vendor dependability constraints.

“The business case for deploying the ASI framework is strong. You’ll improve security, manage vulnerabilities, notice malicious behaviour quickly and continue to protect the infrastructure far more effectively than you would have been able to in the past. It should really form the basis of any long term security strategy.”

He advises that organisations that want to deploy the ASI framework need to start small. “Select a small project around for example guest access or a wireless project and demonstrate the success to the business first. Early wins will enable you to broadcast the success of the framework to the entire organisation.” says Van Vuuren.

Case in Point

The Challenge

Dexia was born out of the 1996 alliance of the two major European players in local public finance: Crédit Local in France and Crédit Communal in Belgium. Dexia forms one of the first cross-border mergers in the European banking sector, which is today one of the top fifteen banking groups in the Euro zone. Dexia employs close to 24,000 staff in 22 countries across all 5 continents.

Carlo Trausch, Network Team Manager at Dexia says, “As a result of unauthorised, unmanaged external laptop computers using Dexia’s network, we became increasingly at risk of virus and worms infections. These potential threats led Dexia to take proactive measures to decrease the risk and avoid the following potential impacts: business disruptions, additional costs and productivity losses.”

The Solution

To fulfil Dexia’s requirements, Dimension Data implemented the Adaptive Secure Infrastructure (ASI) framework, an IT security risk programme. The framework envisions security risks and challenges and assists Dexia to improve security of its networks in Belgium and Luxembourg, facilitating more than 20,000 users.

Trausch says, “Dexia is now in a position where we can grant external visitors controlled access to our network without putting IT assets at stake. Costs are controlled as helpdesk calls are reduced and SLAs ensure improved network/device availability and reliability.”



Regional Head Office Contact Details

Africa

The Campus
57 Sloane Street
Bryanston Sandton, 2191
South Africa
Tel +27 (0)11 575 0000
Fax +27 (0)11 576 0000

Asia*

6 Shenton Way #24-11
DBS Building, Tower Two
Singapore 068809
Tel +65 6322 6688
Fax +65 6323 7933

Australia

121-127 Harrington Street
The Rocks, NSW 2000
Australia
Tel +61 (0) 2 8249 5000
Fax +61 (0) 2 8249 5369

Europe

Dimension Data House
Building 2, Waterfront Business Park
Fleet Road, Fleet
Hampshire GU51 3QT
United Kingdom
Tel +44(0)1252 779000
Fax +44(0)1252 779010

United States

One Penn Plaza
Suite 1600
New York, NY 10119
Tel: +1 212 613 1220
Fax: +1 212 563 7279

*trading as Datacraft Asia Ltd