As we progress through 2013, it’s essential to dispel some basic – and widespread – IT security-related misconceptions that could easily lead to distraction, assumptions or ill-advised investments… or even see you heading down a path that leaves your organisation vulnerable to security breaches or attacks.

“IT leaders are confused, some even ‘paralysed’, unsure of how to adjust and update enterprise security in line with the new devices entering the workplace and modern working styles. At the same time, many fear that these developments call for a large-scale technology refresh – for which most businesses have no budget, given the current economic climate.”
Myth # 1: An effective enterprise mobility strategy calls for a ‘rip-and-replace’ approach.

Reality: While the consequences of a poorly planned and reactive BYOD response can be grave, developing a proactive strategy for secure enterprise mobility presents an opportunity to revisit security approaches that no longer serve the business well, and to update obsolete policies – without necessarily starting from scratch.

The security policies in place at many businesses today were written at a time when the typical mobile fleet consisted of laptops that were corporate-issued and fully locked down. That’s simply no longer the case, with today’s workers using independently-purchased iPhones, iPads and other mobile devices to perform their jobs. In some cases, the current shift from company owned devices to BYOD is being implemented in a phased approach or, in some cases, being balanced with a ‘choose your own device’ strategy, to deliver the best of both worlds.

According to Anna Watson, Dimension Data’s General Manager for Security Solutions in Europe, the result is that many IT professionals are currently in a state of limbo:

“IT leaders are confused, some even ‘paralysed’, unsure of how to adjust and update enterprise security in line with the new devices entering the workplace and modern working styles. At the same time, many fear that these developments call for a large-scale technology refresh – for which most businesses have no budget, given the current economic climate.”

Watson believes it’s not about ‘ripping and replacing’. She explains that as a first step, businesses need to go ‘back to basics’ and review their underlying security policies.

“The focus now needs to be on the data – not the device,” she explains.

“The device is little more than a tool to connect to the data or services that workers need to be more productive. The shift in the security industry from protecting the device to protecting the data is certainly a welcome one. Enterprise mobility is a great starting point because it is something very tangible. But you need to look at the bigger picture, which includes the data centre, the applications and even the network which users have access to.

Then you can review policies and see what the risk really is.

“The upside is that you have a chance to review what’s already in place and adjust it to a new environment. Accurate planning is the way to do it and it actually represents a great opportunity to revisit out-of-date policies and ensure employees can be productive while data remains secure,” she adds.

Myth # 2: Cloud security is mature and well understood.

Reality: The industry is a lot less mature than many think. Now’s the time to understand what cloud security really means for your business and put a well thought-out plan in place.

With so much noise in the marketplace around cloud computing there’s a misconception that organisations have a firm grasp on what cloud security actually means and that today ‘everything’ is well on its way to the cloud. In reality the industry is a lot less mature. Right now, cloud security is a topic that seems to be raising more questions than answers.
At present, businesses are typically in the early stages of prioritising which workloads to move to the cloud and are taking their first, small steps. They’re focusing on consolidation and standardisation in their own data centres while keeping a sharp eye on costs. As organisations implement virtualisation in their data centre environments there’s a natural, initial loss of visibility and control. However, security technologies are evolving to assist businesses plug any gaps.

There’s also a great deal of confusion about what it means to secure a cloud environment and deliver security in – and from – the cloud. We’re not just playing semantics – there are different aspects to cloud security. We need to be specific about distinguishing between security of the cloud, security in the cloud and security from the cloud.

In its simplest form, security of the cloud is about how secure a cloud provider’s cloud offerings – private, public and hybrid – are. It’s about how zealous the provider is about internal security as well as the security of the applications through all layers of a multi-tenant or dedicated environment.

Security from the cloud involves using cloud infrastructure to deliver your own security operations, for example monitoring and correlation management from the cloud.

Finally, there’s security in the cloud. Previously organisations had on-premise content security solutions, performing e-mail or web security onsite, many are now ‘cloudifying’ these security applications by purchasing cloud-based security elements from a vendor. Here, the issue of data sovereignty regulations specific to certain countries or regions must be thoroughly considered.

If you haven’t got a firm grasp of all the different nuances, you could find yourself in hot water.

Also important to bear in mind is the fact that any client’s journey to cloud involves an immense amount of change around their process, risk thresholds and use of technology. Dimension Data’s primary concern at present is maintaining – if not improving – the existing security controls its clients have in place as they chart their journeys to the cloud.

**Myth # 3: Threats are becoming more advanced.**

**Reality:** Threats are not necessarily becoming more advanced but they’re becoming more targeted. Criminals are becoming more savvy, using less obvious methods and increasingly exploiting the ‘human factor’.

Some years ago the major risk an e-mail account user may have faced was a dubious-looking message from a supposed banking representative, requesting (typically in broken English) that the customer confirm his or her banking details by clicking on a link. For businesses, the most likely source of a security breach or data loss would be a dishonest or disgruntled employee tossing a USB stick out an office window to an awaiting accomplice.

While times have certainly changed, threats today are not necessarily more advanced. However, perpetrators are becoming more cunning, and their efforts more targeted.

The human factor has always represented a security risk but now it’s moving front and centre. For example, given the smaller screen interface of mobile devices it’s more difficult for users to judge whether or not an e-mail is safe to open or a website safe to enter. Increasingly, cybercriminals are targeting social networking sites. The reason isn’t hard to fathom: people are typically more relaxed and less guarded when using these sites than they would be, for instance, when doing their Internet banking. Today, a common approach on the part of criminals is to send Facebook users a message to the effect of “Your Facebook friend Bob thinks you’ll like this link”. Knowing and trusting Bob, you don’t hesitate to follow the link – and potentially end up giving out personal information that could be used to defraud you.

In days gone by, employees’ only source or provider of applications was the IT department – today, we all know that’s no longer the case. ‘Bad apps’ is an area of growing concern. Like social media sites, application stores are also relatively soft targets as users are typically unwary when downloading applications from an online store.

Another interesting shift is that criminals are now targeting individual ‘soft targets’ in order to hack into large businesses’ IT networks. An ‘average’ employee – one who does not necessarily have the ability or desire to access confidential company intellectual property – may think they’re not an attractive target (after all, most people are more worried about forgetting their login password than someone hacking into their computer!). But don’t always think of yourself as criminals’ ‘end-goal’ – unwittingly allowing them to access your data will open the door to the risk of data loss or leakage for the business further up the chain.

**Myth # 4: The industry is serious about combatting cybercrime.**

**Reality:** The security community still needs to do more work on the collaboration front to share intelligence so that we can all stay one step ahead of cybercriminals.

Today, as part of their efforts to keep the threats posed by cybercriminals at bay, most businesses have security monitoring tools in place; in fact, most will have more than one security vendor’s products installed. You might assume that the wealth of information these tools collect every day is pooled and shared among security vendors with a view to converting it into useful security intelligence. You’d be wrong.

In fact, there’s disturbingly little evidence of forums or industry bodies that collectively, convert information gathered into much more powerful intelligence. So when is the industry going to start working together to merge their intellectual property for the greater good? After all, technologies themselves from the various vendors often already interoperate. Where does the responsibility lie? Is this a moral discussion?

Perhaps we as an industry should call on all key players to be more proactive regarding their findings before the clients we serve fall victim to potentially devastating incidents that could have been avoided.