

| Open for Business

security for the real world

a white paper from LANZen - secure information solutions |

<http://www.lanzen.co.uk>

Security for IT systems has always been something of a black art for business people. You know you need it, but is it actually protecting your business properly - or is it just getting between you and your customers?



Let's take a step back for a moment. Visualise your business. First, as bricks and mortar. With products or services you show to your customers and with other things you need to keep to yourself, like your bank details, company accounts and internal business processes.

Now, think about your IT systems. How are they secured?

Does your IT security mirror your business model - or is it something that's been simply wrapped around your business like a fence or wall. The chances are it's just a wraparound. It's called perimeter security. It's what most businesses have always relied on to protect their systems - *and it's simply wrong!*

Not convinced?

OK, let's look at it this way. Imagine you run a bank, or a business with high value items you want to sell, like a jewellers. You place the business in a good location like a busy high street. People - your potential customers - pass your business every day, browsing in the window and coming in to do business with you.

It's easy to design security for this, isn't it? The frontage of your business would be made open and attractive. People will stop to look. In the public area of your business, it's open, warm and inviting. You're free to move around and interact with your customers and they have a clear view of what you're offering them.



The back office or vault, however, is secured. The customers can't get in, but you can pass to between this area and the public area freely. Common sense has dictated that this area is protected.

Now, clearly you've not been told anything new here. It's the most logical way of doing business and no one would dream of doing it any other way. So how come conventional IT security gets it so wrong?

Why perimeter security alone is bad for business

Telling you that most companies have implemented security wrongly in their organisations may seem a very bold thing to do. How can the combined skills of so many people be wrong?

To answer that, we need to go look once again at the security design of the average IT system. Remember, this was meant to be designed for *your* business. Problem is, the choice of security product was probably left to an IT security person with little consideration for your business, or simply tacked on from information some IT security company gave you to sell their product. And all it really consists of is a fence around the outside of your business. Worse of all, it's stopping you more than the people you want to protect against!

Let's go back to the same bricks and mortar environment we discussed, but this time, picture the result if conventional IT security practices were applied to the physical security of your business in the same way as your IT system. It's not pretty!

At the end of the street, he's built a tall, barbed wire fence. The street looks like a war zone. Everyone who walks towards your shop is stopped, searched and interrogated. The bad guys have secretly snipped a hole in the fence and slipped through, while you and your customers - the legitimate users - struggle to get in.

The really silly thing is, once inside the perimeter there is no specific protection for the back office or vault where your secure data actually is, because the security has been placed around the perimeter instead!

If you ran your business like this, you simply couldn't trade, nor would even want to.

Why accept this for your IT systems - which are now just as much a part of your business as your bricks and mortar?



LANZen implements IT security for the real world.

LANZen recommends security is implemented to emulate real life. We do this by establishing something that mirrors how you do business called *security zones*.

The first zone is an outer zone, or OZ. hosting your web site or store frontage - open, inviting. This is the public area. Not restricted at all, just helpful and guiding.

Next zone is the shop area, or banking hall itself, where you actually trade. This gives your clients what they want, but not what you don't want them to have access to. Behaviour in this area is more managed. This is what we call the DMZ. The middle, neutral ground. Your public facing systems live here.

Finally. The inner zone. Your data storage or back-end server area - like your back-office or vault, sits inside this. Protected heavily, this area has strict rules for entry and removal of information or business assets, available to trusted people only.

Unlike conventional perimeter security, which tries to draw a circle around your business, that has to stretch further getting weaker as your business expands and constantly costing you more, a centric or cored zone approach concentrates on your inner information area, continuing to protect your business as it grows.

By protecting your assets specifically, the most effective and best value will be returned from your IT investment. But more importantly, your business will be secure to trade freely in the real world. And that's what business is really about.

Talk to LANZen and build a secure information solution for your business.

Call 01260 290 592 or mail info@lanzen.co.uk today.

Visit the LANZen web site regularly for other news and information

<http://www.lanzen.co.uk>