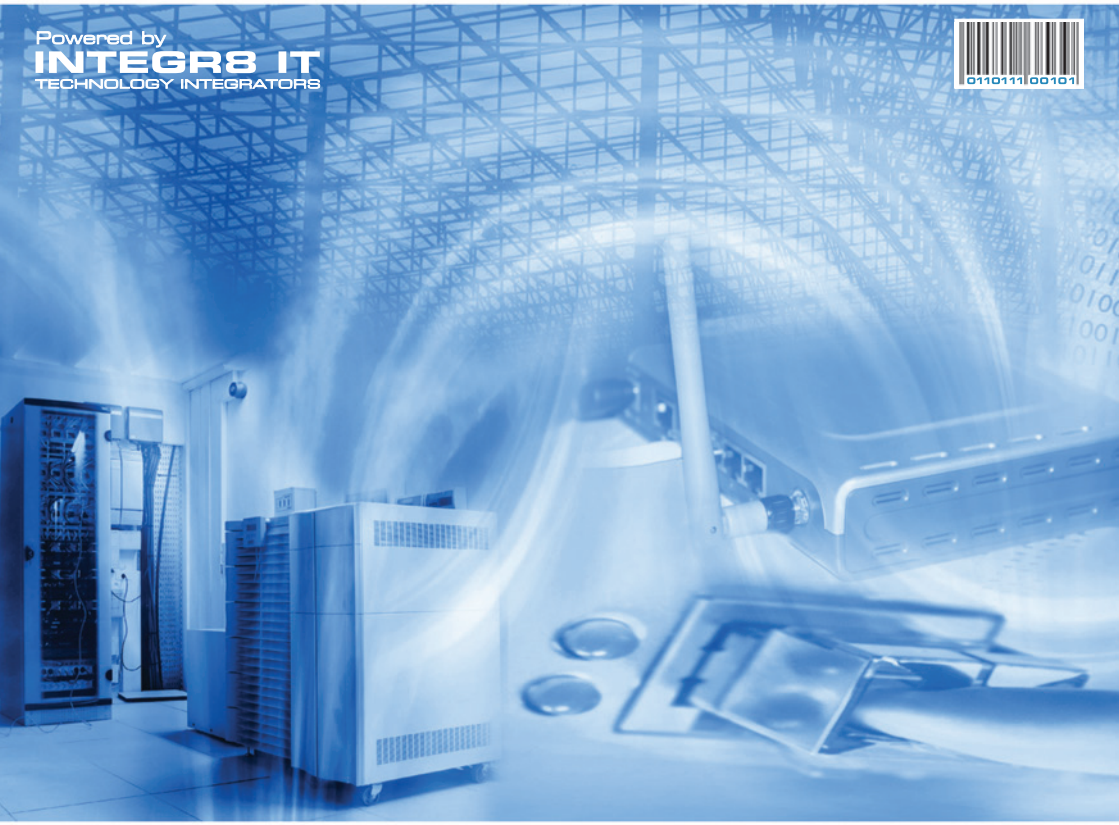
SECURITY

Powered by
INTEGR8 IT
TECHNOLOGY INTEGRATORS



SECURITY AUDITS

ACCESS TO THE BEST VENDORS

PHYSICAL SECURITY INCLUDED

CLOUD SECURITY LOCKED DOWN

INTEGR8
GROUP

Zero day attacks have become all too prevalent and when even the biggest ICT companies like Google are themselves compromised, CIOs around the world are asking one key question: "Am I safe?"

It's not surprising that even during an economic slowdown, spending on security outpaces all ICT spend and multiple global surveys place security as the number one concern for CIOs.

Integr8 takes its security offerings very seriously, spending hundreds of hours ensuring our intelligence is absolutely current so we can protect our clients.

A basic level of security is no luxury. An unpatched system will be compromised by hostile code within minutes of direct Internet connectivity, and an unprotected network perimeter will be quickly exploited by attackers.

Malware and hackers are recognised threats, which should be controlled at an operational level. Security mechanisms such as the authentication and encryption provided by a virtual private network are universally considered to be mandatory for remote access to sensitive internal systems. These are the baseline requirements for any company – and yet they are not so easy to provide.

An organisation in doubt over the integrity of their security systems should ask themselves these key questions:

1. What is the status of my security technology?

At the very least mature security solutions, such as firewalls and antivirus software, should have been implemented by organisations and operationalised or outsourced so that the enterprise can focus on critical needs.

2. How do I balance risk and cost?

The expense of not implementing security can be the cost of mitigating a problem, such as a viral outbreak, system downtime and revenue loss because customers lose confidence. Be sure you know what your risks are and how much they may end up costing your company.

3. What new or updated regulatory or legal requirements do I face?

The legislative and compliance landscape is changing constantly. And while only lawyers have the time to understand all the requirements, we all know that ignorance is not a defence. At the very least ensure your company is aware of various personal privacy legislation and compliance issues.

4. What standards and best practices affect my technology?

These are in flux, and while the IEEE and other bodies work frantically to ensure harmonisation, companies will have to assess what they use and if these are sufficient on their own.

It is clear just from these four questions that security is an aspect of ICT management that can keep multiple staff members busy on a fulltime basis. It is for this reason that Integr8 has cherry-picked the industry's leading minds in security and we can ensure that your company is protected. Call one our many offices to speak to a security expert who will guide you through the nuances of creating a secure environment for your business.