And finally . . .

- Awareness often provides the best "bang for the buck"; simple education programs can improve security quickly and effectively.
- Simplify and standardize wherever possible; remember that complexity is the enemy of good security.

Data

Unless you have specialist needs – like protecting plant or production equipment – then it's all about protecting the data

- Most businesses need to be able to collaborate and thus you should actually design to "leak" data, but in a secure manner.
- Legitimate data will "leak" using many routes – from Web to email, USB sticks to FTP transfer – what you implement must be holistic and match your business needs.

  Remember: Implementing many disparate products that just block (or worse still, require your partners to have the matching software) will generally not meet the needs of the business.
- Ideally, data security needs to be inherent with the data or using a specific secure protocol relevant to the data (not an IPSec tunnel). Security at the network layer should be about providing Quality of Service and not protection of the data.

References and where to go for further information

1. The Jericho Forum® Commandments, a good quick (only two sides) read: www.opengroup.org/jericho/commandments_v1.2.pdf
2. The Jericho Forum® Self-Assessment Scheme: www.opengroup.org/jericho/SAS_Guide.pdf
3. Cloud Security Alliance version 2.1 if you are looking at cloud computing: https://cloudsecurityalliance.org
4. The Information Security Awareness Forum directors guides: www.theisaf.org/kzscripts/default.asp?cid=9
5. Data protection guidance: www.ico.gov.uk
6. ISF Good Practice Guide: www.isfsecuritystandard.com

Infosecurity Buyers Guide

In this issue

Before you arrive

Are your info-security fundamentals in place?

- Both IT fundamentals and the business fundamentals

What are the current business priorities?

- Today, 6 months, 12 months and longer

What is the business strategy?

- What do you need to align with to support this strategy?

What is the businesses collaboration strategy?

- Think about joint venture, suppliers, vendors, and other partners
- Think about how you collaborate with them
- There will be more than you realise!

Where is your data?

- Where does your business need it to go?
- Remember: By default, data must be appropriately secured when stored, in transit, and in use.

What is your Mobile Strategy?

An introduction from the editor

This guide has been produced for InfoSecurity Europe in conjunction with the Jericho Forum®. It is not a definitive reference guide to buying security products; rather it is intended to give you some key pointers to what you may want to look at and some of the "nasty questions" to ask the vendors as you navigate the show.

Paul Simmonds, April 2011

Get the fundamentals right

Do you understand what's on your network?

- What each device is?
- What state it's in?
- Who is the business owner?
- Who is responsible for managing it?
- How vulnerable it all is?

Do you understand the connections to the outside world?

Do you understand how your users/partners/joint ventures interconnect to you and your data?

Do you really understand everywhere your business uses its corporate data?

Do you know what's <u>not</u> on your network?

- Mobile devices/laptops. Etc. that you own and should manage
- Mobile devices/laptops, etc. that you don't own but consume your data
- Access to email from home computers
- Consumerisation of IT
- Cloud-delivered services
- Outsourced services and/or tasks
- Third-party data processors

Do you understand the interaction between different systems and their data?

Implementing my new solution

Installation

- Who's going to install the solution?
- Can installation be automated?
- How much installation will we have to do manually?

What level of training on the solution will the users need?

Encryption should be mandatory, but who will manage the encryption keys?

Living with what I buy

Who is going to provide ongoing management?

- Who will care, water, and feed the solution?
- Maintenance patches and upgrades?
- Errors, outages, and general problems?

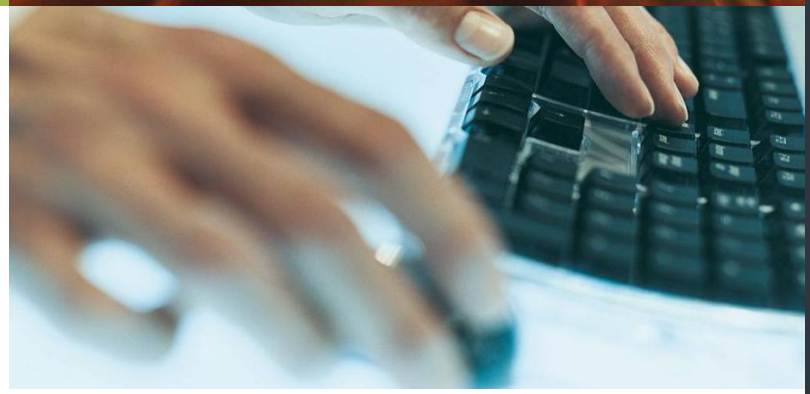
Will your existing management system manage all of it, or do you need yet another management system?

What will happen when you have more than just PCs to manage? Will it expand to Macs, iPads, Android, Blackberry, or the next big thing?

If you have logs and alerts how will you manage them, review them, and respond in a timely manner?

What a first-time security manager really needs to prioritize

We asked some of the leading CISOs for their top tips



Question to ask yourself (or your prospective vendor)

How do we manage user identity? Is it cradle to grave?

- Is it with one or more systems?
- If so, which ones?
- Are they compatible?

How do we manage privileged users?

How do we manage non-employee users?

Can we expand this identity to all the devices we manage?

Are our security mechanisms pervasive, simple, scalable, and easy to manage?

Do we use ***only*** secure protocols?

Will it work identically on the Internet, and be secure?

Will any new solution work in OUR context?

What can I eliminate?

Tip #1
Review what you already have and eliminate old products and obsolete products where possible; if you are ripping out competitor products often vendors will offer extra discounts.

Tip #2
Most of the basics can be done at either no cost or minimal cost.

Outsourcing and Software as a Service (SaaS)

Outsourcing or using software as a service is often seen as a great solution. And often it is, but we forget the basics of outsourcing at our peril.

- Don't outsource what you can't properly define, or don't outsource a mess and hope your vendor will fix it.
- Understand how you will monitor and measure effectiveness of an outsourced service.
- How will you know if you are successful?
- Understand and document, up front, how you will exit the contract.
- Understand where your data is, and how you will retain the data in the event of "exit for cause" or if the provider goes bust.
- Understand where your data is being held and how it's being secured.

Top Security Improvement Tip

Many products have security built in; for example, Windows 7 will encrypt both the hard disk and USB keys if you buy the right version.

Remember:

"You can try and outsource a problem, but you can't outsource liability"

Measuring the effectiveness of security

There is an old management adage "if you can't measure it, you can't manage it".

- How will you measure the effectiveness of the product or service you buy?
- Always look to be able to provide an ROI (Return on Investment) calculation.

Be very sceptical of any vendor who comes with a "canned" ROI calculation for you to use.

In my experience this often indicates that the product is very expensive and the returns are dubious!

Improve what you already have

Most products have some security built in, but often not switched on!

Ask your existing vendors how they can improve the security posture of their products.

The better vendors should provide this help and guidance free as part of the annual maintenance fees they charge.