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
3. Cloud Security Alliance version 2.1 if you are looking at cloud computing: https://cloudsecurityalliance.org
5. Data protection guidance: www.ico.gov.uk
6. ISF Good Practice Guide: www.issecuritystandard.com

Copyright © 2011 Jericho Forum®. All rights reserved. Jericho Forum® is a registered trademark of The Open Group.
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?

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.

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.