


<http://www.info4security.com/story.asp?sectioncode=10&storycode=3093822&c=1>



User Area
User Name
Password →
[Forgotten Password?](#) [Register](#)

I4S HOME SECURITY INSTALLATION SECURITY MANAGEMENT IFSEC CCTV IP & NETWORKS GUARDING INTRUDER ALARMS ACCESS CONTROL REFERENCE

News Ticker: [Security Management - Teenagers 'well advised' to use pseudonyms onli...](#) [Security Managem](#) →

- News
- Features
- Opinion
- Products
- Regulation
- Legislation
- Industry Groups
- Management Skills
- Campaigns

- Events
- Subscribe
- Awards
- Jobs
- Contact Us
- Media Pack
- Advanced Search

Secure IT

Are you PCI compliant?

11 Jun 07

By **Jon Shaw**

Organisations affected by the Payment Card Industry's (PCI) Data Security Standard – which comes into force later this month – and who are looking to comply with its recommendations should be aiming to exceed the six basic mandates. How might they do so? Jon Shaw investigates.

With a stringent set of criteria to meet and such a tight deadline looming, security managers and IT security directors may already have taken the view that Payment Card Industry (PCI) compliance is an ass! Come the end of this month, thousands of organisations across the UK will have been driven by a hefty stick. The big question is... are there any carrots?

Compliance deadlines have a tendency to spread fear, uncertainty and doubt rather than promote the inevitable improvements they are designed to deliver. Ask 100 random people to describe their first ever car and I'll bet their responses will be littered with the term 'death trap'. Fortunately, an individual's extinction just because their car is rubbish has become a thing of the past as modern safety laws mandate higher minimum standards for side impact protection and crash tests, etc. Manufacturers that cannot meet the standards will not be able to sell their product to market.

As far as the PCI is concerned, the compliance bar has been set high from the start, so the challenge for retailers and payment providers to differentiate themselves by accelerating away from compliance uniformity has not been straightforward.

Organisations whose businesses are dependent upon meeting the PCI Data Security Standard by the end of this month have much to gain – and nothing to lose – by taking another two steps forward. They should be more positive about the additional commercial and operational benefits to be derived by meeting PCI compliance now, and grasp this fundamental opportunity in their IT infrastructure life-cycle to build a near-term plan that will exceed the PCI Data Security Standard's requirements.

Considering the benefits

In terms of PCI compliance benefits, variables like: "Avoid \$500,000 per compliance breach fines" and "Keep from being blackmailed by Visa, MasterCard et al" don't count. There are real business advantages enabled by the development of an IT infrastructure that meets the PCI Standard.

The man-in-the-street credit card holder might not know that you only just squeezed past the post on the compliance deadline, but your suppliers and business partners will. Don't delay. Impress them and your bosses! It's unlikely that you'll choose to market your PCI pass grade credentials to customers. Given that it's an extremely robust standard, perhaps you'll not need to. Customer confidence lives or dies on the back of public perception, but you can plan ahead to ensure there's no PR disaster waiting around the corner.

The closer the deadline, the more 'in demand' specialist IT contractors will be. With compliance under your belt, you needn't burden your budget with £2,000-per-day 'gunslingers'. Your staff will be grateful that they can spend the summer of 2007 with no sign of wild panic in the background.


Exceeding the PCI's security mandate

There are six main areas of the PCI Data Security Standard, representing a total of 12 individual requirements.

"The essential message to all organisations affected by any regulatory

In terms of building and maintaining a secure network, this calls for a firewall configuration that prevents internal interfaces from connecting to external ones. Security and IT managers can exceed their remit here by implementing the

Click on images



Jon Shaw

External weblinks

Info4Security is not responsible for the content of external internet sites.

- [Ingrian Networks](#)



<http://www.info4security.com/story.asp?sectioncode=10&storycode=3093822&c=1>

compliance is this: "If you fail to plan, you plan to fail". That is the 'guiding principle' behind the PCI Data Security Standard. There is no 'PCI-in-a-box' solution""

802.1X Standard. This will strengthen the user access control capabilities of all wireless LAN networks.

The protection of cardholder data is often referred to as the 'Black Hole' of PCI compliance. Establishing strong encryption for data in transit, as well as at rest, is where most organisations struggle, let alone exceed. Strive for maximum cryptographic throughput – preferably via a dedicated hardware appliance – and safeguard the entire process with

centralised key management. Store level encryption is the ultimate goal (ie encryption at the Electronic Point of Sale, in store).

Always strive to maintain a vulnerability management programme. Organisations should ensure that there are effective procedures in place to identify, categorise and flag-up any potential malware threats. By doing so, IT and security managers can combat threats before they become problems. This is being proactive as far as security is concerned.

Look to implement strong access control measures. By instigating two or three factor authentication, companies can ensure that access to sensitive data remains a privilege and not a right. By asking the end user to employ "something they know" (such as a password) and "something they have" (for example, a swipe card) admission control is greatly strengthened overall.

Regularly monitor and test all networks. In addition to the relatively straightforward practices of network monitoring and testing, organisations should partner with an independent auditor that can show accreditation and proven experience in the field. Moreover, you should partner with an auditor certified to validate compliance to all portions of the PCI compliance program.

Last but not least, always maintain an information security policy. Ensure that all interested parties and Stakeholders are involved in the conception and development of effective security guidelines. This can help to ingrain security into the organisational ethos and prevent unnecessary incidents from occurring due to uncertainty or ignorance.

Fail to plan, plan to fail

The PCI Data Security Standard provides the impetus for organisations to evaluate their existing security capabilities, identify any areas of weakness and put into effect a plan that will strengthen their abilities. This will help to future-proof the company, not only against further compliance requirements but also current and emerging security threats. The standard is an alarm clock, rather than being a mere wake-up call.

The essential message to all organisations affected by any regulatory compliance is this: "If you fail to plan, you plan to fail". That is the 'guiding principle' behind the PCI Data Security Standard. There is no silver bullet or 'PCI-in-a-box' solution for adherence. Companies need to possess a suite of technology in order to cover all potential vulnerabilities in their security provisions.

Security managers and IT security directors will then be able to look to the future and spot challenges and opportunities rather than always having to look over their shoulder.

Postscript :

Jon Shaw is EMEA Region sales manager at Ingrian Networks (www.ingrian.co.uk)

[Top](#)

E-mail sign-up Please sign me up for the following news services:

- Info4Security Daily Digest Info4Security Weekly Digest IP & Networks Platform Editor's View Security Installation
 Security Management SI Editor's View SMT Editor's View

[Sign up here](#)

© Info4Security 2007 | [Contact Us](#) | [Feedback](#) | [RSS FEEDS](#) | [Terms and Conditions](#) | [Privacy Policy](#) | [CMP Information](#) | [Site Map](#) | [Publication Index](#) |

Visit our other websites at: [Building](#) | [Building4Jobs](#) | [Property Week](#) | [PropertyWeek4Jobs](#) | [Building Design](#) | [BD4Jobs](#) | [QS News](#) | [QS News4Jobs](#) | [Regenerate](#) | [Building Services Journal](#) | [BSJ4Jobs](#) | [Construction Manager](#) | [Electrical & Mechanical Contractor](#) | [Property Direct](#) | [Riba Journal](#) | [Safety & Health Practitioner](#) | [SHP4Jobs](#) | [Whats New in Building](#) | [Zerochampion.com](#) | [Barbour ABI](#) | [Barbour](#) | [Barbour Compendium](#) | [The Interior Design](#)