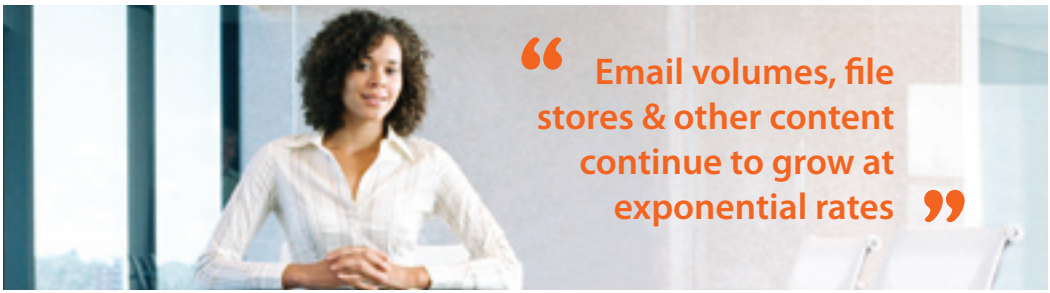
Summer 2008

Information & System Security Newsletter

## *Email Archiving*




IDC research[1] forecasts that enterprise storage requirements will be increasing by 50-60 per cent a year for the next few years, creating major challenges for organisations in almost every business sector.

In this context, **Symantec Enterprise Vault** has already established itself as the 'no compromise' intelligent archiving solution – with Symantec positioned in the Leaders Quadrant of Gartner Inc.'s Email Active Archiving Magic Quadrant[2].

Symantec Enterprise Vault 2007 is the latest release of this product and reinforces its credentials with file life cycle management to help free up even more space while reducing overall storage requirements and keeping content fully searchable and instantly accessible.

This is supported by active policy management to archive, migrate, delete or block content based upon its profile. Also available are advanced reporting, profiling and categorisation for no compromise management of your data – whichever information system it is from. And for easier integration with your current messaging systems there's advanced support for the new Microsoft 2007 products.

Importantly, Symantec Enterprise Vault 2007 also makes it even faster, simpler and more cost-effective to meet your compliance, investigation or legal discovery needs through its centralised archive and enhanced tools. To find out more about email archiving or to receive either of the documents below, please email **grace.kelly@cstl.com**

**1:** The State of Storage Industry: Growing Pangs and Opportunities, Dave Reinsel, Director Storage Hardware Research, IDC, 2006.
**2:** Gartner Magic Quadrant for E-Mail Active-Archiving Market, Carolyn DiCenzo & Kenneth Chin, May 16 2007

**Key subjects covered in this edition**


- *Email Archiving*
- *Payment Card Industry*
- *Improving Your Security*

## Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) applies to all organisations that transmit, store, or process customer card data on their own network as 'merchants'. It was introduced by the payment card industry collectively to protect cardholder data and reduce the card providers' level of risk from credit card fraud and is enforced with fines and sanctions for noncompliance.

Merchants are classified as levels one to four depending on the volume of transactions processed annually and the overall responsibility for compliance lies with the merchant even where business processes and IT has been outsourced.

## Requirements of the Standard

The standard applies to all payment acceptance channels, including bricks-and-mortar, mail, telephone, e-commerce and encompasses twelve requirements based around administrative controls, physical security and technical security.

## Achieving & Demonstrating Compliance

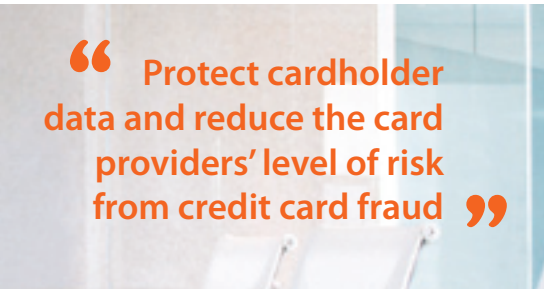
All merchants are responsible for ensuring they comply with the standard by undertaking a formal annual audit process which is recorded and must be produced in the event of security breach. The audit process is conducted through a self assessment questionnaire for merchants processing less than 6 million transactions per year. Merchants processing over 6 million card transactions per year must be audited annually by independent 'Qualified Security Assessors' (QSA) accredited by the PCI Standards Council.

'Approved Scanning Vendors' (ASVs) accredited by the PCI Standards Council must conduct the mandated security testing for all merchants processing over 20,000 e-commerce transactions per year which is also recommended for all other merchants.

### Preparing for Compliance: Top Tips

**Ken Munro Managing Director of SecureTest has provided us with his knowledge and expertise in the payment card industry:**

- **Plan ahead and start early**
  Compliance and remediation may require 6 to 18 months' work
- **Self-evaluate how prepared your own IT and data security controls are**
- **Consider engaging a QSA for a more comprehensive review & deeper education**
  Their experience could well save you time and money Limit the scope of your PCI validation – consider who really needs to 'touch' credit card data Start with solid security policies
- **Initiate discussions with your partners as soon as possible**




## Requirements of the Standard

**Build and maintain a secure network**
Install and maintain a firewall configuration to protect data. Do not use vendor-supplied defaults for system passwords and other security parameters.

**Protect cardholder data**
Protect stored data (use encryption). Encrypt transmission of cardholder data and sensitive information across public networks.

**Maintain a vulnerability mgt program**
Use and regularly update anti-virus software. Develop and maintain secure systems and applications. Implement strong access control measures. Restrict access to data by business need to-know. Assign a unique ID to each person with computer access. Restrict physical access to cardholder data.

**Regularly monitor and test networks**
Track and monitor all access to network resources and cardholder data. Regularly test security systems and processes.

**Maintain an information security policy**
Maintain a policy that addresses information security.

**To receive more information about PCI audit and security recommendations please email grace.kelly@cstl.com**

## *New Team Members*

To further augment our professional security services, Martin Stevens has been employed as IT Services manager with overall responsibility for the whole of the services team. CST would like to welcome Ben Bridgman who will be fronting the support team providing senior support and consultancy. We also welcome

Daniel Frayn who will be providing first line support and in-house expertise. Our new members ensure that customer service quality and response times improves.

## *Webcasts*

CST are hosting weekly webcasts about Symantec Endpoint Protection and Symantec Network Access Control. If you would like to attend one of these webcasts please email **grace.kelly@cstl.com**

## *CST Evolves*

As you may have noticed, our appearance and company logo have changed. We invite you to check out our new look website at **www.cstl.com** where free product evaluations are on offer along with new security solutions.

We also provide new security methodology

information in our new corporate brochure. If you would like to receive a copy or arrange a consultation with CST, please contact us today.

## *Improving Your Security*

CST (Computer Security Technology) has over 11 years of IT security expertise, exclusively and distinctively specialises in network and information security. We provide consultancy and managed services for IT departments who may lack the time, resources, or expertise themselves. CST is here to compliment your own resources and help fill any resourcing and skill gaps within your own security posture.

CST is keen to build and maintain robust relationships with customers; we feel it is important to have a good level of trust as we work with sensitive customer information. CST's typical customer engagement commences with a project based security assignment, in time this leads to mutual trust and confidence which in turn results in CST typically becoming a trusted adviser for objective advice and pragmatic assistance, all of which is independent from any security vendor and delivered without the industry rhetoric.

> "No single vendor or product can secure your business.
>
> One independent specialist can."

# Data breaches will cost you your reputation and money

**CST is offering you a consultation to discuss your data issues**

- Data Loss Prevention
- Encryption
- Network Access Control
- End Point Security

Call Grace Kelly on 020 7621 7832
Visit **www.CSTL.com/Encryption**
to register your interest today!