HE Update - January 2017

Payment Card Industry – Data Security Standards

What is PCI - DSS?

The notorious US criminal Willie Sutton, when asked why he robbed banks, reportedly replied 'because that's where the money is!'. The same logic applies to electronic fraud in the 21st century, with card payments growing rapidly every year and customer data therefore increasingly vulnerable to theft. Weaknesses can appear at any point in the card-processing cycle, including point-of-sale devices, PCs or servers, mobile devices, network infrastructure and paper records.

The Payment Card Industry - Data Security Standards (PCI–DSS) were introduced in 2006 by the Security Standards Council of the Payments Card Industry to combat fraudulent use of payment (credit and debit) card details. All merchants accepting card payments need to demonstrate ongoing compliance. The standards are worldwide and cover security of the transmission, storage and processing of customer's payment card details. These include:

- ***operational controls*** such as: restriction of authorised users, physical security of point-of-sale payment devices, secure retention and disposal of receipts, user education to prevent recording of card details;
- ***IT security controls*** such as: firewall settings, network configurations and access controls.

Implications for Universities

Universities will receive card payments for a variety of services including catering, retail, accommodation, student fees - and often a wider range of services such as car parks, and online stores. The compliance criteria that a merchant such as a University has to meet are set by the individual payment brands, and the merchant's 'acquiring' bank e.g. BarclayCard. Each payment brand has its own compliance programme and divides merchants into one of four 'levels' based on the volume of transactions and other criteria such as whether the organisation has been breached before. A 'Level 1' merchant will have a more stringent compliance than a 'Level 4' merchant, who may typically be required to complete a self-assessment questionnaire.

Although compliance with PCI-DSS is mandatory, it is not enforced by law. However, penalties are applied by the individual payment brands and the severity of these measures depends on the number of transactions the organisation processes. It would likely comprise a monetary fine per transaction across the institution, a burdensome increase in security auditing, and potentially losing the ability to process card transactions altogether. Clearly there is also the reputational damage that would ensue from a breach.

For institutions, the first stage is to understand and define the 'cardholder data environment' (CDE) - i.e. the areas where payment card processing takes place. This will allow the University to ensure that all staff in those areas are adequately informed and trained, and ensure that card processing equipment, data and networks are adequately secured.

The central department responsible for PCI-DSS (in many organisations this will be the Finance Department or its equivalent) will have a key role in defining the CDE and ensuring all relevant staff and management are aware of, and following, relevant standards. There will also be a need to work closely with IT and legal departments to ensure appropriate policies are in place, and to work closely with third parties (e.g. outsourced caterers) and card acquirers.

The IT department will need to manage and secure the relevant University networks where card data is processed, stored and transmitted. The standards outline six best practice security steps which need to be in place:

- Build and maintain a secure network and systems
- Protect cardholder data
- Maintain a vulnerability management programme
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy.

Some Common Issues

A close relationship between Finance and IT is vital. Finance must have assurance that the relevant network and system components are protected adequately. Liaison should be ongoing (e.g. via a working group of all interested parties, with clearly-defined ownership) because payment systems and related security measures will be subject to frequent change.

Problems may originate with staff 'on the ground'. Many staff accepting card payments will be casual (e.g. in catering outlets or sports facilities) and remote from central university oversight. All staff must be fully informed of security policies and procedures and trained adequately.

Uniac Approach

In addition to complying with mandatory requirements of the acquirer (such as a specialist audit of completion of self-assessment questionnaire) a periodic internal audit will help to review how the main PCI-DSS compliance risks are being managed and to suggest areas for improvement.

Uniac staff have attained 'PCI Professional' accreditation. Our audits of PCI-DSS will include:

- sample checks of local areas processing payments
- reviewing staff knowledge of PCI-DSS requirements, training, security procedures and practices e.g. device and paper records
- financial and operational controls, physical security, retention periods
- IT security controls and policies.

Get in Touch

If you would like to discuss how Uniac could help provide assurance over PCI-DSS risks and controls, please contact:

Ian Musgrave - Head of IT Risk and Assurance
PCI Professional Accredited

☎ 0161 247 4697

imusgrave@uniac.co.uk