

How to stay safe from cyber crime

By Jason Walsh

Una Dillon, spokesperson for the Irish Payment Services Organisation (ISPO), said that major Irish retailers were aware of their liabilities and the fines that could be levied by the payment card industry (PCI).

"PCI compliance is hugely important. We can see that criminals will primarily target larger retailers due to the higher volume of transactions, but that doesn't mean smaller business are immune to attack," she said.

Dillon said that a key issue for smaller retailers was to understand that PCI compliance was an ongoing process and one of constant evolution. According to ISPO data, €16.5 million worth of fraudulent transactions occurred in Ireland last year, and €15 million the year before. Others estimate the loss could be closer to €100 million.

Despite the overall rise, Dillon said the figures indicated a decline. "It's going down in terms of per transaction. The volume of transactions increased during that period," she said.

PCI compliance is required of all merchants using Visa and MasterCard, and there is an onus on the bank that supplies the merchant account to inform the retailer of this. However, PCI compliance itself is the responsibility of the individual business doing the card processing.

"It's mandatory. Whether you love it or hate it, you have to do it," said Jon Morris, from British-based IT security consultancy Ambersail, which works with clients across Europe and elsewhere to ensure PCI compliance. "Basically, it's a scheme put together primarily by Visa and MasterCard that works to combat credit card fraud," he said. "It's based on the ISO 1799 standard, which is best practice for IT security."

"The over-riding body is the PCI Security Standards Council. It develops the standard and ensures that organisations like ourselves, which help to achieve compliance, are measured."

In order to obtain PCI compliance, a merchant must ensure that their network is secured and tested, that access to data is restricted technically and physically, and that transmissions are encrypted. There are four tiers to PCI compliance, each relating



Michael Conway, of Dublin-based IT security firm Renaissance

to a volume of transactions annually.

Tier one is for businesses that process more than six million transactions. Tier two is for those that process one to six million. Tier three is for businesses processing 20,000 to one million, and tier four is for those that process below 20,000. Tiers three and four are self-assessed regimes, whereas tiers one and two require external validation.

"The risk is higher [for tiers one and two], so a more comprehensive audit is required," said Morris.

Merchants in tiers one and two must have a quarterly scan of their systems, and it must be performed by a PCI authorised service vendor (ASV).

Erban Schrott, of anti-virus company Eset, said that businesses should be aware that they needed to protect themselves not from the traditional image of lone hackers, but from international organised crime.

"Cyber-criminals are there to make money, it's as simple as that. Credit card numbers sell in volume for as little as 5 or 10 cent per number. Eighty per cent of regular criminals get caught, but less than 10 per cent of cyber criminals currently do," he said, noting that international borders were a particular problem.

"Companies that handle large volumes should be aware of the need for indepen-

dent assessment, and there are Irish and EU standards for this," said Schrott. "You are, as a business, responsible for data belonging to your customers," he said, adding that one simple virus on a system was enough to breach security.

Michael Conway, of Dublin-based IT security firm Renaissance, said: "It's not about products. It can include products but it's more an issue of a mindset and knowledge base." He said that not enough businesses were taking security seriously.

"There was a car park in Dublin that, until very recently at least, printed your entire credit card number on the receipt," he said.

"The PCI standard doesn't protect the user, in the sense that it deals with the financial impact but not the other side of data loss. You lose data through negligent retailers not doing their job, not usually through yourself. They're also not being sufficiently guided."

Dermot Williams, of Threatscape, said PCI compliance could be misunderstood. "Hardcore security people will remind you that just because you're compliant doesn't mean you're completely secure. There are no silver bullets in IT security," he said.

"On the other hand, it does raise the bar to such an extent that hackers will move on to another target. A lot of PCI is what people should be doing anyway."

PCI compliance checklist

PCI compliance requires the following 12 rules in six specific areas.

1. Build and maintain a secure network

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

2. Protect cardholder data

- Protect stored cardholder data.
- Encrypt transmission of cardholder data across open, public networks.

3. Maintain a vulnerability management programme

- Use and regularly update anti-virus software.
- Develop and maintain secure systems and applications.

4. Implement strong access control measures

- Restrict access to cardholder data by business need-to-know.
- Assign a unique ID to each person with computer access.

- Restrict physical access to cardholder data.

5. Regularly monitor and test networks

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

6. Maintain an information security policy

- Maintain a policy that addresses information security.