PCI Compliance up 20% from 2014

The number of organisations that fully complied with the payment card industry (PCI) security standards during 2014 rose to 20%

The number of organisations that fully complied with the payment card industry (PCI) security standards during 2014 rose to 20%, according to the latest Verizon PCI compliance report. Previous reports showed that in 2013, only 11.1% of companies worldwide were fully PCI compliant, with average global compliance rising to 93.7% in 2014, up from 85.2%. The report indicated that the level of full compliance was due to an improvement of compliance across the board, with over 60% of organisations assessed during 2014 compliant with any of the 12 PCI DSS requirements. As a result, PCI DSS compliance went up by an average of 18% for 11 out of 12 requirements. *Adam Winn, Manager of OPSWAT states that " PCI-DSS is sometimes considered the poster child of effective an compliance program, and for good reason. Payment processing is a ripe target for attackers, as the payouts can be substantial for a successful attack. Consumers have a lot of direct control over where they spend their money, and in what format they spend it, and they also have a very real and direct connection to payment processing risks. There’s a tangible connection to security when a consumer completes a transaction. This type of awareness creates a competitive environment where companies must

maintain a high level of security, perceived or actual. This is in stark contrast to other industries. Specifically healthcare and HIPAA. Consumers often lack any or all choice when it comes to selecting their health care provider. Hospitals and doctors do not advertise the security of their medical records systems, and consumers rarely consider the very real financial impact of medical record theft. For this reason, there's comparatively less industry and consumer pressure to improve the state of HIPAA technical standards." Andrew Wild, CISO at Lancope provided the following further insight; "As has been said many times over, security is a process, not an end state. IT environments are very dynamic in nature; both security and compliance require very thorough processes to ensure that an organisation's IT environment remains secure and compliant. Many organisations do not have the processes in place to ensure a proactive security posture and are stuck in a reactive mode, constantly trying to keep up." The fact that post breach investigations have shown that breached organisations were not compliant at the time of the incident is an indication that achieving 100% continual compliance across an entire organisation is very challenging. The number of payment breaches in 2014 is more of a testament of the fact that criminal organisations have become very adept at monetising IT vulnerabilities, using both simple and advanced exploits to gain access to payment card data. Compliance should be viewed as the minimum requirement, but compliance doesn't ensure adequate security. Security should be implemented with an approach based upon risk management. Absolute security isn't likely something that can be achieved, so organisations must prioritise the resources available to implement security based upon an assessment of the risks they face. This has to be a ongoing process, and different organisations will have different risk tolerances and consequently, will have varying levels of security implemented. I found the four recommendations from Verizon to be very interesting (page 7), particularly recommendation #2 "Focus on Scoping". I agree strongly with the focus on scoping. Organisations must understand their environments, and work to minimize the scope of their payment card environment. However, reducing the scope of the payment card environment can be a difficult task, especially for organisations that haven't implemented a strong asset management system, and haven't implemented adequate network segmentation."