



As we begin to settle in on the New Year, security remains a hot topic. Already we have seen breaches of large companies, such as JCPenney, where thousands of consumer's have had their data compromised. 2007 was a record year and 2008 is not missing a beat.

Over SecureState's tenure, our consultants have recognized various trends each year. To better assist future planning our consultants have decided to release the Top 8 Trends they see having the largest impact on budgets, decisions and consumer confidence for the next 12 months.

- 1) **Web Application Security**- Application security becomes “mandatory”, effective June 2008 per the rigid Payment Card Industry (PCI) Data Security Standards (DSS). We believe other regulations and audit procedures will follow suit. In addition to web application security, the PCI Council is reported to have incorporated new Payment Application Data Security Standards. This now forces proper secure coding practices in the SDLC, a welcomed addition to the security front. We also see a significant increase in the popularity of Web Application Firewalls; specifically, Cisco is releasing a new updated firewall mid year. We have also seen software based firewalls entering the market, with Applicure being a low cost but effective solution.
- 2) **Convergence of Logical and Physical Security**- When the United States Government passed the Homeland Security Presidential Directive 12 (HSPD-12) in August of 2004, it raised awareness and defined the importance of incorporating a single Personal Identity Verification (PIV) system. With only a fraction of the United States Federal Agencies hitting the targeted date of October 2006 (two years later) for compliance, this clearly demonstrates the divergence between physical and logical access control. We have had discussions with a number of organizations that are looking to build a process that is similar to what is used by the government to comply with HSPD-12. Cisco and other companies are discussing “smart building” systems that will move all facility systems/devices (HVAC) to be Internet Protocol (IP) based. While we believe this to be a convergence, we don't see a significant investment in securing these systems/devices. With the convergence, we should see the birth of companies embracing a single point of security; i.e., a Chief Security Officer with reporting capabilities for both physical and logical security.
- 3) **PCI Compliance Focus on Level 2-4**- PCI Council and card brands have been pushing compliance for all levels of merchants and service providers since June 30, 2005. Surprisingly, only 65 percent of Level One merchants (those processing six million transactions per year) reported being fully compliant (“September 2007 Compliance Report,” Visa). The remaining levels two through four top out at 55 percent compliant. The primary focus will certainly be to continue compliance efforts with level one and push heavily on levels two through four, with acquiring banks becoming more involved with the compliance efforts.

- 4) **Okay, After Eleven Years We Are Finally Ready for HIPAA-** It appears that the first HSS audit last year (July 2007) of a healthcare provider has sparked renewed interest in the HIPAA federal regulation. While HIPAA has been around since 1996, very few organizations have embraced the requirement fully. We have seen a significant increase in organizations requesting HIPAA Readiness Reviews, to properly document the gaps in their current state of security and create a mitigation plan to meet compliance. We anticipate that most healthcare providers will start to become compliant as early as 2009.
- 5) **Outsourcing Your Risk (We mean Security)** – As Managed Services continue to grow, corporations will have more and more core business components managed by outside companies. Specifically, most corporations believe that their Service Level Agreements (SLA) with these vendors mandate security controls be implemented. While this is rarely the case, we believe a shift in industry will focus on service providers as a source of security, and companies will need to enforce their security requirements at these entities. We also believe that many of the current service providers (specifically hosting companies and web design companies) will look to build security into their processes and environment. However, this will not be included in their current fee structure!
- 6) **Globalization of Security-** The ability for organizations to capitalize on markets outside the United States has been increasing and will continue to increase the competitive landscape. However, these new markets are opening US based companies with new threats. As such, a distributed security organization will be spawned, working in conjunction with Audit and Legal departments, with oversight from Risk Management.
- 7) **Security Structure — Dude, is that our CISO?** – Companies will continue to make investments into security; however, a shift from low level security resources to higher level decision makers with the ability to drive change and manage risk will become a requirement. Specifically in 2007, several Fortune 500 companies have hired their first CISO, with other organizations of similar size following suit. Keeping with the managed services theme, security companies are providing “Virtual Chief Information Security Officer” (VCISO) services that allow organizations (generally less than one billion) to build an enterprise security organization pulling from a team of experts rather than one person.
- 8) **Unified Approach to Security-** As more and more regulations continue to affect companies in various industries predicated on data being stored or processed (such as energy companies and the new North American Energy Reliability Council’s Critical Infrastructure Protection standards), companies will start to develop a unified security program. The unified security will develop a comprehensive approach to look at all applicable security, privacy and other regulatory requirements. We have seen companies mapping requirements between HIPAA, PCI, GLBA, state laws for Data Breach Disclosure and the European Union’s Directive 95/46/EC on the protection of personal data to the ISO 27001/27002 framework (formally 17799), with full compliance to the outlined controls (estimated 770+ specific control requirements).