Level 3, 66 King Street
Sydney NSW 2000 Australia
Telephone +61 2 9290 4444
or 1300 922 923

Business Opportunity
Enablement through Information Security Compliance

E-commerce waits for no-one; unlock your company's full potential by demonstrating information security compliance ahead of the pack.

The days of trusting that customers, suppliers and business partners had security systems capable of protecting your business' most vital asset – its information – are over, giving those that can demonstrate adoption of industry and best practice information security standards a huge competitive advantage.

Compliance is set to be the buzz word of the new decade. With increased freedom in what we do and how we do it, regulation and compliance have become the discipline of our day. Protecting information – our own and that of others – is crucial. Mismanaging it can cost dearly – loss of reputation, loss of business opportunity, loss of income and loss of status. In some cases, loss of entire business. It's that important.

Compliance has previously been driven by government – which, having spent the time, money and effort required to protect the sensitive information it holds, is no longer willing to do e-business with companies that don't meet the stringent ISO 27001 and 27002 standards.

The compliance mandate is now moving out from government agencies to large corporations. Essentially, organisations that have their security organised are demanding that those they do business with also comply … or lose the opportunity to conduct that business.

Furthermore organisations that store, process and transmit Payment Card (Credit Card) Data will trigger the need to demonstrate compliance with the Payment Card Industry Data Security Standard (PCI DSS). Within the PCI DSS, the banking industry is currently undertaking education of smaller entities as to what their responsibilities are under this Standard. Larger companies which hit the PCI DSS trigger need to be compliant by September 30, 2010 or face fines. So non-compliance will cost them money, reputation and opportunity.

"81 percent of organisations subject to PCI DSS who experienced a data breach in 2008 had not been found compliant prior to the breach."
Verizon 2009 Data Breach Investigations Report

Australia's 25-year old National Privacy Act is currently before the Federal Government for review. It is understood that a breach notification requirement is to be introduced, so that anyone whose details are leaked (whether inadvertently or maliciously) will henceforth be informed of that leak. It is therefore incumbent upon organisations to take appropriate measures to ensure

"81 percent of organisations subject to PCI DSS who experienced a data breach in 2008 had not been found compliant prior to the breach."

Verizon 2009 Data Breach Investigations Report

the confidentiality of information held on their systems can be maintained. A Privacy Commissioner is to be appointed who will have the power to levy fines.

The coming National Broadband Network is also set to change the compliance landscape. As more bandwidth becomes available, more services will be provided electronically and regulatory rigour will increase.

For now, compliance is a huge selling point for companies that do comply … since many companies are either ignorant of their responsibilities or, more sinisterly, trying to skirt them.

Today, compliance is a commercial reality. Tomorrow, companies will be unable to conduct e-business without it. Compliance isn't an IT issue, it's one that affects your business' very future.

To be ahead of the game, control costs by undertaking the changes that need to be made in a methodical fashion - one that's applicable to your needs. Not everyone needs the same level of information security; you can do it on your own terms. Implemented systematically, compliance enables business opportunities and avoids the unseemly haste and error points of trying to work to someone else's deadline

Responsibilities? What responsibilities?

Few companies today think they are underspending on IT. There are many, however, which are overspending … and still not achieving a reasonable level of information protection.

According to the IT Policy and Compliance Group (IT PCG), organisations now rank the loss of confidentiality and integrity as the top two business risks, followed by loss of availability.

The ITPCG has ongoing benchmarks measuring three key performance results:

1. Loss or theft of customer data
2. Incidence and extent of business downtime from IT failures and disruptions
3. Deficiencies in IT that must be corrected to pass audit

The best results are experienced by only 13 percent of organisations. Annually, these companies endure less than three losses or thefts of sensitive information, less than six hours of business downtime and less than three deficiencies to correct to pass audit. Those are the best results.

The bulk of companies are experiencing results that are considerably worse - nearly seven in 10 organisations suffer data

"Today, compliance is a commercial reality. Tomorrow, companies will be unable to conduct e-business without it."

loss or theft rates ranging from three to 15 each year, between seven and 79 hours of business downtime and between three and 15 compliance deficiencies in IT that must be corrected. This is the 'normative' group.

Nearly two in 10 organisations - 19 percent - are experiencing the worst outcomes, the highest data losses or thefts, the most downtime from IT failures and the largest problems with regulatory compliance. They experience more than 15 losses or data thefts each year, 80+ hours of business downtime from IT failures and more than 15 IT deficiencies that must be corrected to pass audit.

Interestingly, the financial outcomes being experienced by organisations are directly related to the outcomes being managed within IT.

And while those numbers might make security and compliance sound like an IT issue, the potential exposure to financial loss – and in almost every case, the suffering of actual financial loss – means that this is a whole-of-business issue … and a critical one at that.

The IT PCG says that for businesses with annual revenues of $50 million, having IT practices in the worst group costs them $1.5 million a year; having normative practices costs them $240,000 and having best practices costs them $20,500. Similarly, for businesses with $500 million in annual revenue, worst practices cost them $19 million, normative practices cost $3.3 million and best practices cost $211,000. Every year.

No business can afford to be in the worst category; there are clear advantages to being in the best category despite the initial costs of compliance.

And there are excellent financial returns for IT integrity - companies that are compliant avoid overspending on audit fees and expenses to sustain audit results each year – organisations with the best results can cut their audit fees and expenses by between 35 and 52 percent.

The good news is that the opportunity to reduce risks and costs while improving results is a level playing field – highly regulated industries have no advantage over those with less regulated environments and big businesses have no advantage over small businesses.

Organisations with the worst results and highest losses from the use of IT are actually spending the same amounts on information security as the firms with the lowest risks and best outcomes. It's not about how much you spend; it's about allocating that spend to deliver practices that gain better results.

"Nearly two in 10 organisations - 19 percent - are experiencing the worst outcomes, the highest data losses or thefts, the most downtime from IT failures and the largest problems with regulatory compliance."

"The losses organisations are willing to sustain are exceedingly low and the returns for improving results are extraordinarily high. Loss of confidentiality, integrity and availability are larger business and financial risks than are outsourced IT projects, systems, information or delays to critical projects."

IT Policy Compliance Group

Implementing appropriate actions and practises is the way to improve results and reduce financial risk and loss as well as audit expenditure. Cost control remains paramount; organisations can now achieve the results they need with the budgets they have.

Automating controls, along with continuous monitoring and assessment and managing information around your business' particular risk profile are critical, yet achievable tasks that can move businesses rapidly from worst to best case scenarios.

The ITPCG says that theft or loss of customer data is rated as the highest business risk by more than 72 percent of organisations. It makes sense then to implement practices that reduce that risk to its lowest possible level.

The Payment Card Industry (PCI) is, of course, more highly regulated than many other industries with global representatives from American Express, MasterCard and Visa forming the PCI Security Standards Council which provides guidelines, based on the ISO framework, that acquirers, merchants and service providers must meet to demonstrate compliance.

Non-compliance – what have we got to lose?

There are large numbers of businesses that currently do not even have what may be considered reasonably secure environments. There are several reasons for this –

- The business might not know that its environment is not secure. That is, it could be spending money and doing what it believes is right, but spending in the wrong areas and gaining less than optimal results.
- With such a plethora of choice in the market, businesses might be confused about what to do and have adopted an information approach that tries to bolt security on the back, rather than planning it from the front with the same rigour that's applied to financial products.
- Security is often still seen as an IT issue, rather than a business issue, so the people with the most to lose (MD, CEO and Board Members) are leaving it up to IT (whose main priority can be availability over security), unaware of their real exposure.

"The losses organisations are willing to sustain are exceedingly low and the returns for improving results are extraordinarily high. Loss of confidentiality, integrity and availability are larger business and financial risks than are outsourced IT projects, systems, information or delays to critical projects."

IT Policy Compliance Group

- Some might be aware that the information is not secure, yet may not have considered the implications of their choice. At the very least, mismanaging confidential information almost always leads to reputational damage and reputational damage leads to client departures and difficulty attracting new business, sometimes for years. This can have significant bottom line implications.

Those businesses that do not have a secure internal environment are in no position to protect their own information, let alone anyone else's. Yet to compete in the 21st century, they need to move into conducting business electronically.

What they are finding is that the entities they wish to work with are now mandating demonstrations of due diligence and process around the information flowing between the two organisations.

Businesses need to be able to demonstrate that their service and information is housed in a secure environment which is controlling the assets, otherwise the government, banks, large financial institutions and increasingly, major non-financial-industry corporations, simply won't form alliances with them.

Non-compliance then, has a fairly critical opportunity cost – missing not just the first opportunity, but every opportunity thereafter until compliance is achieved - missing the opportunity to grow the business. All of which means maligned reputation, missed revenue and missed profitability.

In other words, comply or cut and run.

Even Microsoft, giant that it is, is working on this issue. It is now putting its Software as a Service offering through ISO compliance, going through due process. Having newly emerged into the services model as well as their traditional licensing model, Microsoft has realised that it needs to demonstrate that the tools customers will be using to access the SaaS (such as Word and Outlook) will be housed and protected in a secure environment – otherwise potential customers will shop for their service elsewhere.

It's all about building confidence up front, demonstrating that your company takes other people's information security as seriously as it takes its own. Proving your trustworthiness.

This also allows businesses to take advantage of market opportunities as they happen in two ways. First, being ISO compliant can be a proactive selling point when discussing doing web-enabled business. Second, not being compliant will rule you out of doing business with a compliant partner, which will damage your reputation and affect your bottom line adversely. And it won't just affect that one opportunity; from now on, not being compliant will rule you out of almost every web-enabled opportunity.

There are, of course, costs associated with becoming compliant. They are nowhere near as great as the costs associated with not being compliant … and they are not in the same universe as the risks to your business – and your partners' - of not becoming compliant

Compliance creates credibility

Many companies now have taken steps to protect their information assets within the bounds of their own environment. They have appropriate policies, procedures and controls to set standards of protection with information and information security.

Having usually gone to considerable planning, effort and expenditure to make sure their information is protected within their corporate boundaries, they are understandably keen to ensure that it doesn't become vulnerable the moment it leaves their environment.

These are the companies which are now saying to their partners, customers and suppliers – if you can't document the ways in which you will protect our information, you are simply too risky to do business with.

Conversely, compliance gives businesses instant credibility. All other things being equal, it could be the single factor that sways the awarding of a much-needed contract.

Coming to compliance

Sense of Security has been growing rapidly since its inception in 2002. A BRW Fast 100 winner in 2009 and a Deloitte Technology Fast 50 winner in 2008 and 2009, the company is now the foremost independent provider of IT security and risk management solutions to leading companies and government departments in Australia.

Our expertise in assessment and assurance as well as strategy and architecture through to deployment and ongoing management gives us the ability to provide our clients with solutions, not just identification of their problems.

Originally built around providing security testing and ethical hacking (penetration testing) services, Sense of Security has evolved into a provider of strategic security advice, implementing security frameworks and roadmaps and developing compliance programs. As the threat landscape has changed, our service offering has matured, now providing customers with continuous targeted vulnerability management and protection.

All our business functions are retained in-house, leaving our clients with no security grey areas. Sense of Security is regularly invited

"These are the companies which are now saying to their partners, customers and suppliers — if you can't document the ways in which you will protect our information, you are simply too risky to do business with."

to present our findings and insight at Board level; we promote thought leadership at this level to raise awareness of IT security as a crucial business issue – not just an IT issue.

Understanding that compliance is a critical to e-business wellbeing and that new partnership opportunities will be lacking until it is achieved, the path forward is straightforward, starting with a gap analysis.

In a series of workshop meetings, Sense of Security consultants undertake a review to discover how your information moves throughout your IT infrastructure and where your business sits from an ISO perspective, benchmarking your processes and practises, then providing a set of recommendations designed to remediate the issues uncovered. This first step can often be completed in as little as a few weeks.

Following that process and unlike other consultancies for whom security is an additional, rather than a core, service, Sense of Security has the architectural capabilities to provide businesses with a system addressing their recommendations.

Each client business has individual requirements – not all organisations need Department of Defence-level security. But to succeed in this new e-environment, all businesses will need to demonstrate an enterprise risk management strategy including protection of information assets.

Many of Australia's leading businesses entrust Sense of Security with their risk management. If you would like to speak to us about any aspect of ISO compliance or your business' specific needs, please call **Neville Gollan** on **+ 61 2 9290 4453** or visit our website at **www.senseofsecurity.com.au**

Level 3, 66 King Street
Sydney NSW 2000 Australia
Telephone +61 2 9290 4444
or 1300 922 923