
A handwritten signature in black ink that reads 'David Light'.

Hacking^{of}
Financials.

Malware^{is}
Installed.

A black and white photograph of a modern skyscraper with a curved facade, illuminated from within at night. The building is the central focus of the advertisement's main image.

Dramatic reductions in your business costs can begin immediately.

Cost^{savings}
from Security.

The new challenges need new skills.	Section No1.	
<p>Listing of Contents.</p> <p>Summary. Section No1. Costs can be dramatically reduced in long range strategic activities, short range tactical activities and day-to-day activities, but few firms have the in-house skills to do so.</p> <p>Summary. Section No2. Immediate bottom line savings can be made in fewer pure play consultants used and redeploying current staff unskilled in security and risk, back to core, more productive tasks.</p> <p>Summary. Section No3. Pre-emptive bottom line savings can be made using our component based knowledge of your systems and working on thwarting major internal and external attack threats.</p> <p>Summary. Section No4. These current uncertain financial times need a response to cutting costs, but at the same time you need increased security from even more serious electronic threats.</p>		<p>'Security is hard to put your finger on. It does not reside in a particular location and is accomplished through a diverse combination of people, process, and technology controls. Adequate security for any given product, service, or organisation is determined based on tolerance for risk - easy to say, hard to quantify, and constantly changing.'</p> <p>Julia Allen. Senior Member of the Technical Staff, Carnegie Mellon University, Software Engineering Institute, CERT® program.</p>
© Sense of Security 2009.	DavidL@senseofsecurity.com	Page No2.
www.senseofsecurity.com	Proprietary rights reserved.	Version 1.2.

Denial of Service.

Infected with Worm.

Engagement fee is modest to begin the boost to your bottom line.

Deploying Pennies to save Pounds.

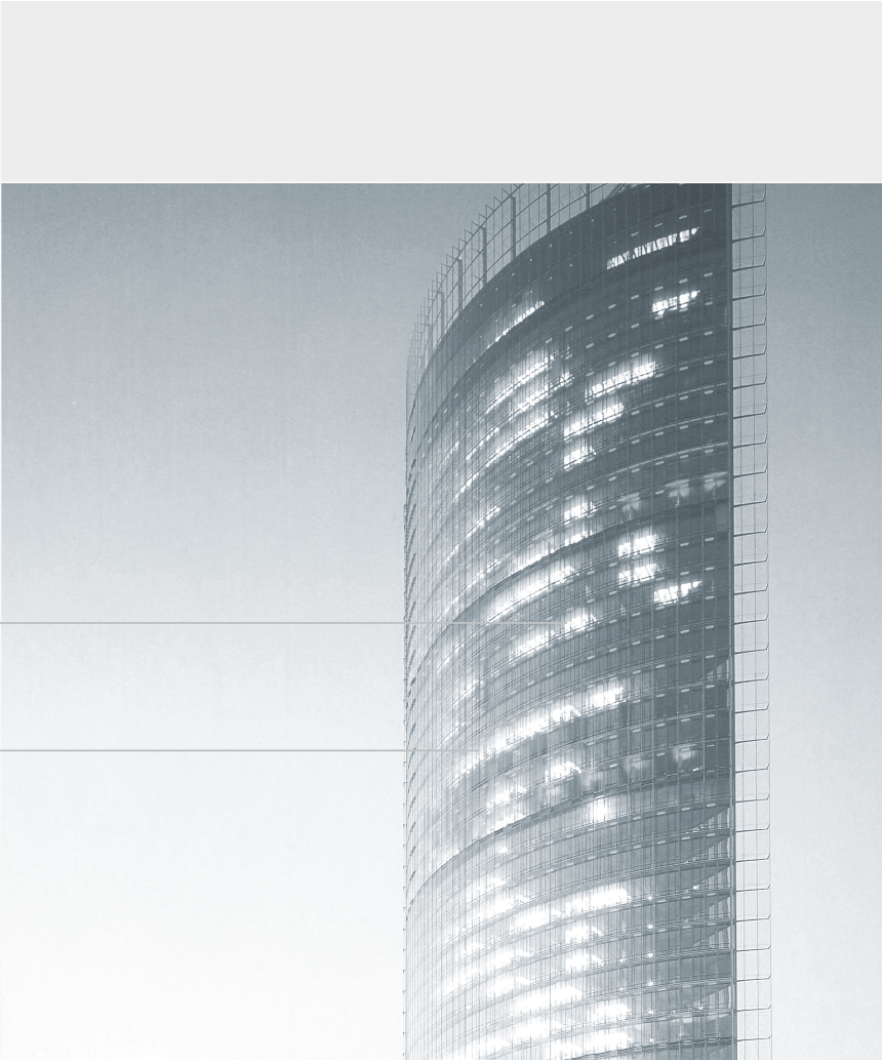
A unique best-of-both-worlds approach.	Section No1.	
<p>Change of any kind is something most businesses rightfully fear as they are simply unprepared.</p> <p>They are unprepared for deciding on how to approach it, how to manage it, and how to measure their efforts.</p> <p>In these fearful financial times those firms with the right mix of high level technology and business skills will be those better equipped to formulate business-wide strategies that address their specific cost cutting needs this very day.</p> <p>They are also the firms more likely to execute successfully on their strategies, and deliver the planned boost to their bottom line.</p> <p>Such firms become revered masters of change, rather than just bullied recipients.</p> <p>Firms looking to cut costs need to look at the opportunities in three very distinct parts of their business, each briefly described in the list below.</p> <ol style="list-style-type: none"> 1. Long range strategic activities, where these would include threat and vulnerability management, security strategy, framework and roadmap, also compliance, governance and information security management, as well as review and development of policies and standards. 2. Short range tactical activities, where these would include securing network, operating system, and applications, also unauthorised access prevention along with business event impact and information risk assessments. 3. Day-to-day activities, where these would include securing access communications and data, also securing data at rest and in transit. <p>In beginning to address the activities noted above many find that they do not have the information technology security and risk management skills in-house to ensure that their cuts do not leave the firm open to far more costly attacks.</p> <p>We have such expertise, such skills. And they can be applied in two areas, securing the enterprise and also preventing a breach, both described in the next two sections.</p>		
© Sense of Security 2009.	DavidL@senseofsecurity.com	Page No4.
www.senseofsecurity.com	Proprietary rights reserved.	Version 1.2.

'Vulnerabilities affecting Web server applications are climbing and so are the attacks, both evidenced by newcomers to the most vulnerable vendor list and this year's automated SQL injection attacks.'

Mark Dowd and John McDonald.
X-Force® 2008 Trend Statistics.
IBM Global Technology Services.

Stealing
credit Data.

Spam_{kit}
Installed.



Some of the current costs saved now in securing the enterprise.

Immediate
line Savings.
bottom

Plans can now become plans of action.	Section No2.	
<p>For an agreed modest budget we can be brought onboard, and the immediate costs that can be saved are removal of the following rather expensive, and now perhaps totally unnecessary consultants. Some are listed below.</p> <ol style="list-style-type: none"> 1. The pure play consultants who just look after one aspect of security like your web site and its back end applications, or VoIP capabilities, or intranet. 2. Consultants advising on privacy regulatory compliance. 3. Online payment system and transaction system advisors. 4. Broad based consultants addressing security without in-depth security skills. <p>We then move on to dividing your business into its working components. This unique method decomposes an enterprise into its discrete zones of trust, systems or activities. This enables our team to list the resources, and exposures, for each component. We can then set to work on each with a deliverable increase in security, and decrease in the cost of security management of that component. We find this component framework is also very useful for communicating with the executive management team giving them clear insight into exactly what is being done, and where.</p> <p>We often find that the component is currently serviced on a manage-by-crisis basis by security skill-lacking support staff. Usually the costs saved here are making crisis intervention unnecessary so staff can be redeployed back to their more productive and profitable tasks. Some of these and other costs saved are listed below.</p> <ol style="list-style-type: none"> 1. High cost staff do not need to be hired or replaced if they leave, we can take over their tasks and ensure continuity. 2. Loss of business if your web site and its ecommerce databases are hacked and offline until reconstructed. 3. Technology support personnel can get back to supporting your staff and the smooth running of your infrastructure. 4. Future costs of fines for non-compliance by regulators, and costs of defence lawyers, and public relations firms. 5. Operations staff can get back to their core tasks. 6. Executive management can once more focus their attention and talents on business strategy. 7. Internet usage bill blow out by install of a spam root kit. 		
© Sense of Security 2009.	DavidL@senseofsecurity.com	Page No6.
www.senseofsecurity.com	Proprietary rights reserved.	Version 1.2.

'There is documented evidence that security breaches can affect brand, marketplace trust, customer privacy and identity, and the bottom line. The proliferation of security laws and regulations demand an increasing share of our attention and effort, with escalating consequences for non-compliance.'

Julia Allen.
Senior Member of the Technical Staff, Carnegie Mellon University, Software Engineering Institute, CERT® program.

Interception
of Emails.

Diversion
of Payments.

Some of the impending costs saved in preventing a breach.

Future bottom line Savings.

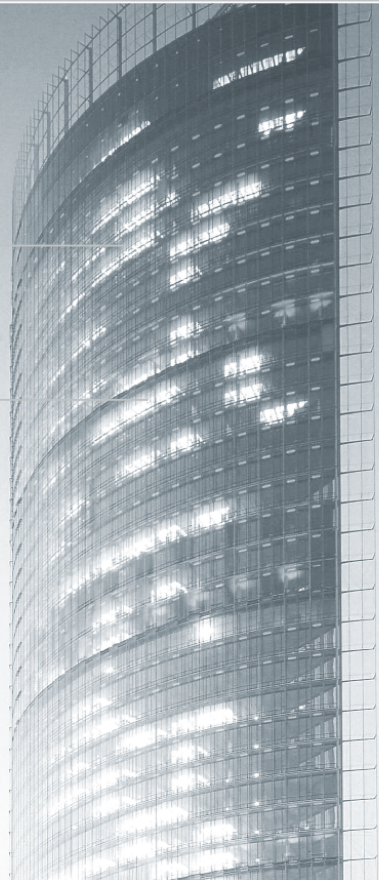
A partnership in skills and communication.	Section No3.	
<p>With our component based knowledge of your systems we adopt a business value perspective of your firm, and work on securing and hardening those parts that would be the source of potentially enormous costs if breached.</p> <p>These losses and costs could be the following.</p> <ol style="list-style-type: none"> 1. Loss of share price if a major breach like credit card details are stolen, or client private information is leaked. 2. Court case from customers whose credit card details have been stolen and have suffered financial loss from the cards being used for transactions by overseas criminal gangs. 3. Loss of income if both your web site and its ecommerce databases are hacked and offline until fixed. 4. Costs of fines for non-compliance by government and industry regulators, and costs of defence lawyers. 5. Loss of consumer confidence from the publicity surrounding a major security breach. 6. Court case costs against internal staff purposely sabotaging your information systems, emails and databases. <p>This use of a business value perspective means that both the executive and technical management both understand the tasks we propose and can redirect our efforts if needed. All decision makers will understand what our team is doing from a future focused point of view, and the quantum of the potential costs to be saved. This is important because often the executive team does not fathom technical logic, but they certainly understand business logic.</p> <p>With all stakeholders understanding the business value of what we are doing this ensures we are working in harmony with your business practices, are contributing each day to your enterprise operation excellence and the intrinsic value of your company is being sustained.</p> <p>As technology changes each quarter, so does the seriousness of threats. Working to a monthly retainer ensures that we are constantly looking at, and thwarting, the methods that external attackers and internal saboteurs will use.</p> <p>Our efforts can then be quantified in both risk management terms, in ongoing corporate compliance and budgets.</p>		
© Sense of Security 2009.	DavidL@senseofsecurity.com	Page No8.
www.senseofsecurity.com	Proprietary rights reserved.	Version 1.2.

'In recent years, Australians have learned about the risk and consequences of data breaches. Well publicised breaches in the United Kingdom and United States brought to light the potential for damage including the loss of customers, difficulty acquiring new ones, and irreparable brand damage.'

Dr Larry Ponemon.
2008 Annual Study: Australian Enterprise Encryption Trends.
The Ponemon Institute.

Intrusion_{of}
Intranet.

Private_{info}
Stolen.



Budgets must be cut, but enterprise security must intensify.

Security_{for}
these**Times.**


An entrusted leap from words to meetings.	Section No4.	
<p>The ability to handle the sudden reduction of budgets, and the parallel need to quickly shore up the enterprise from breaches in security is one of the most profound developments in this decade of business direction and information technology charter.</p> <p>Without the previously loose tolerances of a large budget, the important choice of your information technology security and risk management partner is a process which should rightly put all such candidates under intense scrutiny to ensure they can deliver.</p> <p>We have the track record, credentials and the willingness to become an enthusiastic member of your team and act with quantifiable cost reducing results.</p> <p>But mention of costs that can be identified, targeted and then reduced, are of no help to boosting your bottom line unless something is done.</p> <p>It is now time for your team to decide that the timing is right for both strategic short and long term action, to engage us, and mandate that we begin work on a quickly executable plan.</p> <p>Planning, and then carrying out such plans is something for which we are renowned.</p> <p>It is our hope that here we have begun to gain your trust, and our conversation here begins a rewarding relationship. Should your team need references, you need but ask.</p> <p>We offer our clients a unique approach that can targeted on either discrete security problems, or on wide ranging strategic cost cutting activities, both completed with the deep experience that no other electronic security firm can match.</p> <p>For a plan of action that addresses these uncertain times do call David Light on +61 2 9290 4450. Or if you prefer click on the email link on the bottom of each page.</p> <p>To learn more about us click on the web site link to whisk you to our new site that we are developing.</p>		
© Sense of Security 2009.	DavidL@senseofsecurity.com	Page No10.
www.senseofsecurity.com	Proprietary rights reserved.	Version 1.2.

Head office is level 3, 66 King Street, Sydney, NSW 2000, Australia. Owner of trademark and all copyright is Sense of Security Pty Ltd. Neither text or images can be reproduced without written permission.

Shopping list for an electronic security partner.	Section No4.	
<p>Points to Remember.</p> <p>Summary. Point No1. In these chaotic times those firms with the best technology and business skills will be those most able to carry out cost cutting measures without degrading quality standards.</p> <p>Summary. Point No2. Opportunities for dramatic cost cutting results lie in the three business layers of long range strategic activities, short range tactical activities and day-to-day activities.</p> <p>Summary. Point No3. There are two areas where skills in security and risk management can be applied, costs saved now in securing the enterprise and costs saved in preventing a future breach.</p> <p>Summary. Point No4. Costs can also be saved and recouped by making crisis intervention unnecessary so stretched staff can be redeployed back to their more productive and profitable tasks.</p> <p>Summary. Point No5. A business value perspective assists in discovering those vulnerable business processes to secure and harden so they are not a source of enormous costs if breached.</p> <p>Summary. Point No6. The pressures to reduce costs and at the same time shore up the enterprise from security breaches is one of the most profound developments in this decade for all businesses.</p>		<p>'Web-based vulnerabilities and threats continue to increase. Over the past few years, the focus of endpoint exploitation has dramatically shifted from the operating system to the web browser and multimedia applications.'</p> <p>Mark Dowd and John McDonald. X-Force® 2008 Trend Statistics. IBM Global Technology Services.</p>
© Sense of Security 2009.	DavidL@senseofsecurity.com	Page No11.
www.senseofsecurity.com	Proprietary rights reserved.	Version 1.2.

Hacking_{of}
Banking.

Sabotage_{of}
Applications.



Your information technology security and risk management partner.

Thanks_{for}
Reading.