

# White Paper

## Implications of Outsourcing Web Application Security

# Table of Contents

Implications of Outsourcing Web application security	
Introduction	4/5
On Outsourcing Web Application Security Liability	6/7
Cost Savings of Outsourcing Web Application Security	8
Independence of Outsourced Third Party Web Application Security Audits	9
Conclusion	10
Works Cited	11
About Pacific Coast Information Systems Ltd. & Boonbox	12

## Implications of Outsourcing Web Application Security

"Why should I filter out this garbage at my end?  
Outsource as much of the day-to-day busywork  
as you can, as soon as you can."

- Gartner Analyst John Pescatore

# Introduction

Organizations can never outsource liability for web application security.

As cyber criminals have flourished and the number of attacks on the web application layer by hackers continues to grow unabated, it is incumbent on organizations to ensure web application security. Dozens of security and privacy regulations help guide organizations towards compliance with practices that will help them protect themselves and the people who use their websites and web applications. Total web security can never be guaranteed, but organizations can take steps to reduce the risk.

Executives and managers can safely assume that if they have not specifically contracted a web application security company to ensure their compliance, or have not devoted internal IT resources to it, then they are not web application security compliant.

A common myth perpetuated by managers who may be simply overwhelmed by the complexities of web application security compliance is that they are already outsourcing it and are covered. They may believe that their agreement with their hosting provider or web developer already includes provisions for it.

But it bears repeating that the ultimate responsibility in the event of a security breach belongs with the organization doing the outsourcing, not the company providing outsourced services such as IT web security, hosting or development services. For this reason, it is important for organizations to ensure that the company they choose to carry out web security audits and other security measures must do its work effectively and responsibly.

Put simply, the core business of web hosting companies are to provide secure infrastructure that hosts web applications. They do not have development resources to ensure web applications are secure. On the other hand, web development companies may have web development expertise, but don't typically have web security expertise.

Outsourcing of many aspects of business has been commonplace for decades. Companies understand that significant costs can be saved by using outside specialists instead of attempting to create in-house resources that are not part of the organization's core business.

Now it is common for organizations to outsource aspects of security like web application security.

Web application security is an important component of many organizations' overall security strategy. The consequences of a breach by cyber criminals can be catastrophic to an organization's reputation and bottom line. Meanwhile, the web application layer represents a consistently-growing target for hackers intent on breaching an organization's overall security.

As more and more organizations look to outsourcing web application security, it is important to look at the implications of this action. The implications are as follows:

1. Organizations cannot outsource liability for web application security. Therefore, organizations must be proactive in ensuring that the web application security service provider can prove they are able to provide the highest possible standard of compliance to significantly lower the threat of a security breach.
2. Outsourcing of web application security can lead to significant cost savings compared to dealing with web application security using in-house resources.
3. Outsourcing web application security provides an added benefit of third party objectivity to help organizations confidently present their efforts to industry regulators.

# On Outsourcing Web Application Security

"We've already outsourced security! We have a web hosting service!" This is a common myth perpetuated by managers who have not looked closely enough at their service contract. Hosting companies provide data storage and bandwidth for data transfer.

Hosting companies do not take responsibility for ensuring the HTML code that built your website is secure. It is not part of their core business. The same can be said of website developers, computer technicians and even IT security companies, which may not include web application security service.

Organizations cannot outsource liability. If there is a breach, the company that outsourced web application security is ultimately held responsible – not the web application security compliance service provider (Is Outsourcing an IT Dream or Security Nightmare: a Talk With Ounce Labs" eBiz). This works in the same way that a bank that is robbed cannot sue the maker of its vault that web application security breached with high explosives (or insider information), or the security guard who web application security outgunned.

Thus, organizations must be clear that ultimately, liability for web application security remains with their organization, not the security service provider.

Organizations that wish to realize cost savings and other benefits from outsourcing must be absolutely clear with the security service provider. They must communicate clearly to the contractor what their security requirements are, and must confirm that the security service provider has the technological and logistical capability to fulfill those requirements.

For instance, if an organization requires compliance with the HIPAA set of web application regulations as opposed to more general protection, it is up to the outsourcing organization to gain assurance that the outsourced security solution will do the job.

This is not an onerous requirement; as mentioned, outsourcing application security is already mainstream and best-practices already exist for creating a contract for this ("Outsourcing Turns to IT Security"). It should be stressed that it is up to the company that is outsourcing security to ensure due diligence.

The following checklist may help organizations understand the kinds of questions they should be asking their outsourced web application security service provider:

1. Does the web application security service provider have the expertise and technology to assess your specific requirements? Some web application security solutions focus only on the scans, but these are limited as some vulnerabilities can only be properly diagnosed by human experts.
2. Does your web application security provider have knowledge of web development tools and platforms as well as application security expertise?
3. Does your web application security provider understand the regulatory compliance issues related to your business?
4. How often is testing done? Does this ensure compliance to the specific security regimen that the organization is trying to comply with?
5. Does the web application security service provider have strict policies about how confidential and sensitive material is handled? A web audit scan may reveal information that an organization would prefer to keep confidential.
6. Does the web application security service provider offer web security consulting support to fix vulnerabilities that are discovered? Providing a report on the known security issues is only the first step in making an organization web application security -compliant. The organization must be able to follow up and actually fix the vulnerabilities and deal with them.
7. Does the web application security service provider take the time to understand your business to properly create a roadmap of prioritized remediation steps towards compliance?

The answers that a web application security service provider gives to these questions should provide an organization looking to outsource this function with the answers it needs to make a decision. But the organization must keep in mind at all times that while outsourcing web application security can bring many benefits, outsourcing liability is not an option.

# Cost Savings of Outsourcing Web Application Security

Outsourcing web application security can provide organizations significant cost savings compared with attempting to deliver compliance in-house.

Renowned IT analysts from Gartner could claim as far back as 2005 that outsourcing corporate security is no longer risky and that most organizations would be able to cut costs and improve productivity by outsourcing security services as soon as possible. "It's just not controversial anymore," says Gartner analyst John Pescatore (Network World, "Outsourced Security Called Battle Tested).

Indeed, research by Research Triangle Park International suggests that outsourcing security may have an even bigger cost-savings benefit than from other business functions such as accounting, marketing or human resources management ("Will Outsourcing IT Security Lead to a Higher Social Level of Security?" Brent R. Rowe).

The complex work of manually checking web application code for vulnerabilities to hackers would require a team of specialists working round the clock to ensure compliance. Such work could cost an organization hundreds of thousands or even millions just for IT worker salaries (Pacific Coast Information Systems Ltd. "Calculating Return on Investment (ROI) For Web application security").

Outsourcing of web application security therefore provides significant and immediate cost savings compared with devoting internal IT resources to the problem.

# Independence of Outsourced Third Party Web Application Security Audits

Another benefit of outsourcing that may be overlooked by those focused on immediate ROI is the provision of third party objectivity conferred by the contracted web application security provider.

This benefit for organizations in terms of compliance is akin to that provided by the outsourcing of financial accounting to a specialized accounting firm.

Even smaller firms may have internal access to qualified accountants using respected enterprise-class accounting software. Larger organizations invariably have an accounting department that handles payroll, day-to-day expenses and long-term budget planning.

But even for all of these organizations that have extensive in-house accounting resources, it is still seen as best business practices to have end-of-quarter or annual accounting done by an outside specialist accounting firm. Independent audits are crucial to retaining the confidence of investors and meeting the standards of regulatory bodies like the Internal Revenue Service.

Third-party, independent, outsourced web application security audits by outside specialists are preferred by regulators because they are carried out in an objective manner. The organization's reputation benefits as regulators, investors and clients alike can be confident that the organization is acting in a responsible and businesslike manner.

# Conclusion

Outsourcing security of web applications has become mainstream. The sheer magnitude of threats to web applications coupled with the complexity of dealing with it in-house makes outsourcing security an increasingly popular option.

There are three main implications for organizations considering outsourcing web application security:

1. Outsourcing web application security services does not lead to outsourcing liability. Organizations must communicate clearly to the security service provider their specific needs. In return, the outside contractor must be able to prove to the outsourcing organization that its service will improve security compliance to the highest possible standard to reduce the threat of a security breach. Both sides must do their due diligence to ensure security is provided in an effective manner, although ultimately, liability for security remains with the outsourcing organization.
2. Outsourcing web application security can provide cost savings. It is cost-effective for organizations that do not have the in-house expertise and technology to outsource, allowing them to focus on their core business.
3. Organizations benefit from the independence of a third party web application security audit, comparable to the best business practice of outsourcing financial accounting to ensure confidence of investors, supporters and clients.

Outsourcing web application security allows organizations to focus on what they do best, improve cost-effectiveness and enables competitive advantage.

# Works Cited

Ellen Messmer. "Outsourced Security Called Battle Tested". Network World. 13 June 2005.  
<http://www.networkworld.com/news/2005/061305-outsourcing-security.html>

Mari-Len De Guzman. "Outsourcing Turns to IT Security". IT World Canada. 18 July 2008.

Brent R. Rowe. "Will Outsourcing IT Security Lead to a Higher Social Level of Security?" RTI International. 2007. <http://weis2007.econinfosec.org/papers/47.pdf>

"Calculating Return on Investment (ROI) For Web application security". Pacific Coast Information Systems Ltd./Boonbox. 18 July 2008.

Peter Schoof. "Is Outsourcing an IT Dream or Security Nightmare: A Talk With Ounce Labs". eBiz. 23 April 2008.  
[http://www.ebizq.net/blogs/news\\_security/2008/04/outsourcing\\_an\\_it\\_dream\\_or\\_a\\_s\\_1.php](http://www.ebizq.net/blogs/news_security/2008/04/outsourcing_an_it_dream_or_a_s_1.php)

# About

## Pacific Coast Information Systems Ltd.

Pacific Coast Information Systems (PCIS) Ltd. is a full-service technology and consulting firm based in Vancouver. Founded in 1995, PCIS provides technical assessment & services, business analysis, and IT project management. More information about PCIS can be found at [www.pcis.com](http://www.pcis.com)

## Boonbox

Boonbox, a division of PCIS, web application security created in 2007. Boonbox specializes in productivity solutions that deliver immediate results in support of business challenges like security compliance, password protection and data backup issues. More information about Boonbox can be found at [www.boonbox.net](http://www.boonbox.net)