

# White Paper

## Managers' Cheat Sheet for Web Application Security

# Table of Contents

## Managers' Cheat Sheet for Web Application Security

Introduction	3
7 Questions for Managers	4/5
Conclusion	6
About Pacific Coast Information Systems Ltd. & Boonbox	7

# Introduction

*“When something important is going on, silence is a lie.” – A. M. Rosenthal*

When it comes to making decisions about web application security solutions for business, managers need straight talk from their IT staff.

They need the facts about how a particular solution can help their business and what the implications of moving ahead with the solution are. Just as importantly, they need to understand the consequences for their organization of not taking action. Finally, they need to have the ability to question their IT people’s advice with a degree of confidence.

Straight talk on these kinds of issues isn’t always easy to come by. Managers can face reluctance on the part of their IT people to make changes.

This happens for a range of reasons. For a resource-and-time strapped IT department, adopting new technology or procedures can represent an intimidating amount of effort. Some territorial IT staff may see questions from management about new IT solutions as an infringement on their area of expertise and an implied criticism of their professional knowledge. Will this line of questioning undermine their job security?

Another reason for hesitancy on the part of IT staff is lack of knowledge about newer technology. With technology evolving so rapidly, even the professionals can’t possibly keep up familiarity with all of the latest hardware and applications, much less maintain a confident level of expertise for technology solutions to all business challenges.

A final major stumbling block is that IT experts are not necessarily business experts. Without a firm grasp of business objectives and principles, even highly trained IT workers may not have the grounding to see opportunities to help the business improve its operations, cut costs or improve efficiencies.

Paradoxically, IT professionals, who are usually thought of as the early adopters of technology have significant reasons for putting up obstacles to change.

The Managers Cheat Sheet provides managers with the questions they need to ask in order to get straight answers from their IT experts about web application security solutions that will help their business.

# 7 Questions for Managers

Managers are recommended to refer to this list of questions before consulting with their IT staff about web security. With these questions in hand, they may get better information about their web application security needs, as well as current and projected security solutions.

## **1. Are we liable in the event of a web security breach?**

Many organizations are under the misapprehension that if they outsource web security, they are no longer liable for damages or legal problems in the event of a security breach. This is false. Ultimately, responsibility for web security falls on the organization that owns the website.

If your IT staff waffle on this issue, it may signal a more comprehensive failure to cover your organization's IT security needs.

## **2. What kind of security do we have in place for our web applications?**

If your IT staff tells you the web hosting company deals with web security, you've got a problem. Web hosts provide a physical server for your website and a content management system to run it. They don't typically provide comprehensive web application security. That's not their business.

Additionally, the architecture and software used by hosting companies, if not patched and updated effectively, may also cause problems for an organization even if the web application code vulnerabilities have been fixed.

If your IT people say they will need to check, or they don't know exactly what kind of security is in place, your organization may already be in trouble. Make sure all IT workers are completely familiar with the web security measures that are required. They can't maintain security measures if they don't even know what is currently deployed.

## **3. Does our organization have the right technology and expertise to improve our web security?**

A web audit scanner can drastically speed up the process of checking a web application for vulnerabilities, completing its job in hours, as opposed to weeks or months. Qualified web security experts can check for vulnerabilities that a scanner would not detect. This package of technology and expertise should be able to provide recommendations for fixing known issues and proceeding to deal with them.

They will also be able to check all of the web applications you use for the various security compliance regulations that apply to your organization.

If your in-house IT workers can't do these things, or your outsourcing vendor doesn't mention them, you are not protected. Ensure you have a service agreement outlining security

responsibilities for both sides so your needs are addressed and the vendor can do their job properly.

#### **4. Is our company governed by any kind of laws or regulations?**

There are a wide range of laws and regulations governing requirements for web application security features that will protect website users' privacy and information. For instance, health care providers in the USA must follow HIPAA and government agencies in Canada are regulated by PIPEDA or PIPA. Businesses anywhere in the world conducting credit card transactions are mandated to abide by PCI DSS compliance standards.

If your IT workers aren't aware of the regulations, they will not be able to implement effective security measures to ensure compliance. Ignorance of the rules is not a valid defense in the event of an outside audit.

#### **5. Who assesses our website for vulnerabilities to hackers?**

If the answer is, "we do it internally", then ask them how they do it. Ask to see the reports they are preparing to present to regulators in the event of an audit.

If web application security is outsourced, you'll need to ensure that the company doing the work is absolutely clear about your security requirements in terms of regulatory compliance. Ensure your service agreement outlines clearly the responsibilities of both the company and the vendor to which security is being outsourced.

#### **6. How often is our web application checked for security?**

Security compliance regulations may call for "regular" scans and audits, while others may specify quarterly audits. Does your IT staff know how regularly they are supposed to carry out these procedures? Are they meeting the deadlines?

#### **7. Do IT staff have strict policies about how sensitive and confidential information is handled?**

A web audit may reveal information that the company, or departments within the company, wish to keep confidential. Are procedures in place to protect that information?

# Conclusion

Managers need honest answers from their IT staff about web application security. Since managers are not necessarily as aware of technology trends as their IT staff, the list of questions in this white paper is intended to provide some support for managers to get the information they require.

While the list is not definitive, it should be used as a guide for gathering better information to make decisions on the organization's web application security needs. Ideally, IT staff will be able to answer these questions in a way that reassures the manager that web security is being dealt with efficiently and effectively. However, for reasons stated above, IT staff may be unable to provide the answers that managers require.

If the answers that IT staff provide to these questions seem more evasive than informative, or incomplete than expected, then it is up to the manager to probe more deeply. In some cases, it may be necessary to contract outside consulting in order to get the information required and go over the options that can be deployed to ensure a high standard of web security.

# 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, was 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)