

White Paper

Managers' Cheat Sheet for IT Security

Table of Contents

Managers' Cheat Sheet for IT Security

Introduction	3/4
5 Questions for Managers	5-7
Conclusion	8
About Pacific Coast Information Systems Ltd. & Boonbox	9

Introduction

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

When it comes to making decisions about IT security solutions for business, managers need good lines of communication with their IT people.

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. After all, even the best IT departments are already overwhelmed with end-user support tasks.

Highly trained IT staff may understand the security needs of the organization, but may lack the resources, tools, human and know-how, to proactively carry out necessary planning, much less perform regular assessments, routine patching of systems, physical security, and a host of other related tasks.

In some cases, 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? Managers need to keep these factors in mind when communicating with their IT people, especially during times of economic uncertainty.

Another stumbling block is that IT experts are not necessarily business experts, just as the executive management rarely has the IT prowess to fully realize the role that IT can play. Without corporate alignment, and a company-wide understanding of business objectives, 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.



The IT department must work for to support business objectives, and clear communication with management is key.

The Managers Cheat Sheet For IT Security provides managers with the questions they need to ask in order to get straight answers from their IT experts. This will lead to more appropriate IT security solutions that will help the business.

5 Questions Managers Need to Ask

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

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

Many organizations are under the misapprehension that if they outsource aspects of IT such as network configuration and assessments or web hosting, they are no longer liable, or at least are limiting their liability, for damages or legal problems in the event of a security breach. Possibly but this is unlikely.

Ultimately, responsibility for security and privacy compliance falls on the business that requires the development of a network and online presence.

Your IT people typically are not the ones signing contracts with service providers on behalf of your organization. But as a manager, you must be aware of your liabilities before you sign on the dotted line with any service provider. You have to understand what's in the contract and know your company's ongoing responsibilities to cover off the areas of security that are not dealt with contractually by an outside company.

Your IT people can help you outline liabilities and areas of responsibility. Ensure they are part of the process before your company signs a service agreement that outsources parts of your security. This will help ensure your liability is fully understood within your organization and that steps are taken to cover off those areas.

2. What kind of security do we have in place for our systems?

It's important to ensure your IT people are absolutely clear not just about their own roles and processes in place for your security, but the role of service providers and partners in ensuring privacy and security compliance.

In regards to web security, for instance, 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 typically part of their business. But if you are outsourcing this kind of service, you will want your IT people to answer questions like how to ensure your information doesn't get mixed up with other organizations' database stored on a shared server.

As well, your IT people must ensure your web applications are getting regular code reviews that close off newly-discovered vulnerabilities.

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.

Make sure all IT workers are completely familiar with the IT 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 security?

Bearing in mind business objectives, does it make more sense to use internal resources or outsource certain aspects of your security?

There are excellent technology tools available for network security assessments and web security assessments that can drastically speed up the process of checking for vulnerabilities and recommending patches or upgrades, completing its job in hours or minutes.

As well, qualified network security and 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.

There should be a business case for outsourcing or for keeping things in-house. Engage your IT people to see if you can run your operations more effectively using either method of deployment.

4. What is the IT department doing to ensure our organization is complying with privacy and security laws and regulations?

As responsible managers are well aware, there are a wide range of laws and regulations governing requirements for privacy and security compliance. 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.

IT people are focused on delivering technical solutions to end-user problems. They need to be aware of the regulations so they will be able to implement effective security measures to ensure compliance. It is important for both sides to collaborate and share knowledge with regard to the regulations.

Ignorance of the rules is not a valid defense in the event of an outside audit.

5. Do your IT people have strict policies about how sensitive and confidential information is handled?

A network security assessment or web security assessment may reveal information that the company, or departments within the company, wishes to keep confidential.

Are procedures in place to protect the confidentiality of that information? Whether security assessments and processes are handled internally or externally, the information must receive the same maximum level of privacy protection. Your IT people can be an excellent source for processes and policies that will ensure the privacy and security compliance of your information. It's also up to the business managers to ensure these processes are filtered through the organization.

Conclusion

Managers need good communication with their IT staff about 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. This paper can also serve as a resource for IT people to start a discussion with the business managers to ensure IT processes are in tune with business requirements.

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

If the answers that IT people provide to these questions seem more evasive than informative, or more incomplete than expected, then it is up to the manager to probe more deeply. Likewise, it is up to business managers to read the reports that IT people provide and make use of their expert recommendations.

In some cases, it may be necessary to contract outside service providers in order to get the information required and go over the options that can be deployed to ensure a high standard of security for your organization. In all cases, whether these services are kept in house or outsourced, the key to success is good communication about balancing business needs and security requirements.

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

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