Sample security plan x

Business

The following sample security plan was put together by a fictitious company named Adventure Works. Because of the increasing focus on security in the computing world, the company has decided to review security practices and put together a plan to improve those practices. Adventure Works' needs may differ from your company's needs, but reading through their plan should give you a good idea of the steps involved in creating a good security plan. This plan was developed by Matthew, Managing Director of Adventure Works, in cooperation with other key members of the Adventure Works staff.

About Adventure Works We are a 20-person firm specializing in high-adventure travel packages.

Our staff includes designers, travel agents, sales and marketing personnel, and the administrative team that supports them. The staff also includes the senior management of the business: the co-founders, Matthew and Denise, and the financial controller, Steve. Objectives This security plan is our first. We will take a broad view of the security risks facing the firm and take prompt action to reduce our exposure. Everyone remembers the virus attack we had earlier this year, and we hope to avoid another disaster like that!

However, I hope that by taking a wider view, we may be able to plan for threats we don't know about yet. I realize that we are limited in time, people, and (of course) cash.

Our main priority is to continue to grow a successful business. We cannot hope for Central Intelligence Agency (CIA)-like security, and it wouldn't be good for our culture to turn Adventure Works into Fort Knox. The project team has weighed these constraints carefully in deciding what to do and has

tried to strike a balance between practicality, cost, comfort, and security measures. We are all convinced, however, that doing nothing is not an option.

I am taking responsibility for leading this review and ensuring that all the action items are carried out.

I am concerned about the risks we face, although having reviewed the plan, I am sure we can address them properly. This project has my full support and is a high priority for the business. Circulation Because this document contains important security information, it is confidential. You are requested to keep it under lock and key when not actually using it, and please don’t leave it lying around or make photocopies. We will not be sending this document via e-mail or storing it on the server—paper copies only, please.

The following people are authorized to view this document: •Matthew (Managing Director) •Denise (Operations Director) •Steve (Financial Controller) •Kim (Staff Manager) •Sutton and Sutton (our lawyers) •Jeremy, our outside security consultant Project Team The project team includes: •Denise, project leader •Steve •Kim •Jeremy, advising our staff and carrying out some of the implementation In addition, we consulted with members of staff from sales, marketing, and design to get their feedback about what they wanted and how the plan might affect them. Section 2: Assessment Results

Our assessment has produced the following results. Skills and Knowledge Our technology consultant, Jeremy, is familiar with the whole situation and will be our expert guide. However, we need to internalize as much of this

knowledge as possible by doing as much of the work as we can. Doing so will also help us save money.

Luckily, Steve is an amateur computer enthusiast. He has attended a security training course. Each member of the project team has read the available security planning guides fromMicrosoftand the Internet Engineering Task Force (IETF) in preparation.

The company as a whole is reasonably technically literate, but (with one or two exceptions) they see computers as tools to get the job done and don’t know much about how they work.

Our Network and Systems •Desktops: Twenty-two (one per member of staff plus two old machines acting as print servers) •Laptop computers: Six (one each for the directors, one for Steve, and three for the sales team) •Printers: Two (one high-end plotter and one printer-fax combo unit for general use) •Servers: One (running Small Business Server 2003 and looking after files, the Internet connection, e-mail, and our customer database) •Internet connection: 1. Mbps cable modem connection The server and several of the computers are linked by 100 Mbps Cat5 Ethernet cables. The remainder are linked by an 802. 11g wireless network with an access port. All computers run Windows XP Professional except for the two print servers and two administrative computers, which run Windows 98.

Security We compared each computer against the checklist in the Security Guide for Small Business. We also ran the MBSA. These actions produced the following results: Virus protection: Not present on six computers; not up-to-date on four computers; generally, most users were aware of viruses but

were a bit unsure about what they could do to prevent them. •Spam-filtering software: Many users have begun to complain about spam, but no protection is in place. •Firewall: We thought the ISP's router included a firewall, but it doesn't; so, we don't have one. •Updates: All the Windows XP Professional systems are up-to-date because they were automatically checking and downloading updates.

However, several installations of Microsoft Office need updating, and the Windows 98 computers are not updated at all. Passwords: A random sampling found that most people aren't using passwords at all or had them written on Post-it notes. In particular, none of the laptop computers are password protected. •Physical security:

We had the insurance people in last year, so the window locks, doors, and alarms are pretty good. However, none of the computers has a serial number etched on its case, and we didn't have a log of the serial numbers. We also noticed that everyone, including Tracy and the two directors, are using the same printer, which means that there is a risk of confidential documents being left there by accident.

Laptop computers: All the laptop computers had shiny bags with big manufacturer logos. No security locks. •Wireless networking: We're wide open here. It turns out that we just set the thing up and it worked, so nobody touched any of the settings. The wireless network is open to people who have wireless access capability to snoop on the network or freeload on the Internet connection. •Web browsing: Everyone thinks that having fast

Internet access is a great perk, but they are using it all the time and without much thought to the risks.

Through a content filtering audit (free with Secure Computing), we found that 20 percent of our Web browsing was unrelated to work. We don’t have a policy on acceptable use, and no one is taking any security measures. •Backups: We back up data on the server to a Digital Audio Tape (DAT) drive on a weekly basis, but we haven’t tested restoring the data; unless people remember to copy local files to the server, those files aren’t backed up, which is unsatisfactory. The server contains our primary customer database, so well-tested backups are essential, as is keeping a copy of backups offsite. Assets

Besides the physical property, our main assets are: •Our product designs and marketing collateral •Records of our contracts with vendors •Our e-mail database and archive of past e-mail messages •Sales orders and the customer database •Financial information •Line-of-Business (LOB) software for online booking and reservations •Paper legal records stored in various filing cabinets All these assets are considered secret and should be accessible only on a need-to-know basis.

In addition, they need to be protected and backed up as safely as we can manage.