

# Sample Security Plan: Adventure Works

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 from Microsoft and 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:** 1.5 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 point. 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.

## Risks

We believe the risks break down into four main categories:

- Intruders (viruses, worms, hijacking of our computer resources or Internet connection, and random malicious use). These are the risks that anyone using computers connected to the Internet faces. High risk, high priority.

- External threats (rivals, disgruntled ex-employees, bad guys after money, and thieves). They are likely to use the same tools as hackers, but in deliberately targeting us they may also try to induce members of staff to supply confidential information or even use stolen material to blackmail or damage us. We need to protect our assets with physical and electronic security. High risk, high priority.
- Internal threats. Whether accidental or deliberate, a member of staff may misuse his or her privileges to disclose confidential information. Low risk, low priority.
- Accidents and disasters. Fires, floods, accidental deletions, hardware failures, and computer crashes. Low risk, medium priority.

## **Priorities**

1. Intruder deterrence:
  - Firewall
  - Virus protection
  - Strengthening the wireless network
  - Replacing the four computers running Windows 98 with computers running Windows XP Professional with SP2
  - Ensuring that all computers are configured to be updated automatically
  - Ongoing user education and policies
2. Theft prevention:
  - Laptop computer security
  - Security marking and asset inventory
  - Moving the server into a secure, lockable room
  - Security locks for desktop and laptop computers
3. Disaster prevention:
  - More frequent backups with offsite storage
  - Ensure backup of users' local data
  - Offsite backup of critical paper documents
  - Regularly testing the backups by performing a restore
4. Internal security and confidentiality:
  - Strong password policy and user education
  - Secure printers for accounts, HR, and directors
  - Review security for filing cabinets and confidential documents

## ***Section 3: Security Plan***

After performing our assessment, we have devised the following security plan.

## Action Items

1. Select, purchase, and install a hardware firewall (or ask our ISP or technology consultant to provide one).
2. Enable Windows Firewall on the server and on all desktop computers.
3. Make sure that antivirus software is installed on all computers and that it is set to automatically update virus definitions.
4. Configure computers running Office Outlook 2003 to use Junk E-mail filtering. Select, purchase, and install spam-filtering software on the mail server, if necessary.
5. On the wireless network, disable service set identifier (SSID) broadcasting, choose and configure a sensible SSID, enable WPA encryption, enable MAC filtering, and configure the access point to allow traffic only from the desktop and laptop computers in the office.
6. Replace the four computers running Windows 98 with computers running Windows XP Professional with SP2.
7. Review all machines to make sure that they are fully updated, and set them to automatically refresh those updates.
8. Buy new, nondescript laptop computer bags and locks.
9. Security mark all desktop computers, laptop computers, and their components.
10. Log all serial numbers.
11. Buy and install desk security locks for desktop computers.
12. Find a suitable, lockable room for the server and move it there.
13. Review backup and restore procedures. Ensure that user data is either stored on the server or copied across regularly prior to backups. Implement daily backups. Ensure that a full backup goes offsite once a week. Ensure that the backup is password protected and encrypted. Review paper documents, and make photocopies for secure offsite storage of critical documents.
14. Configure Small Business Server 2003 and individual machines to enforce reasonably strong passwords. Discuss with users what would be an acceptable balance of convenience and security. (We don't want them writing down their new passwords.)
15. Configure workstations to log users out and require a password to log on again if the workstation is idle for more than 5 minutes.
16. Buy cheap printers for accounts, HR, and the two directors so that they can have private documents printed securely.

## Policy Changes

Kim will update the staff handbook to include new policies on:

- Acceptable use of e-mail and the Internet
- Use of passwords
- Who can take company property away from the office

After she has completed a first draft, it will be reviewed by the directors and the company's attorneys before being rolled out.

## **User Education**

We expect to give up to two hours of user training in small groups as a result of these changes. Training will cover:

- The importance of security
- Passwords
- Laptop computer security
- Virus prevention
- Safe Internet browsing
- Updating software and operating systems from a server
- Introducing the new staff policies
- Making sure employees understand the consequences for not complying with policies
- Assessing employees' understanding of the new policies
- Periodically reviewing the practice of the new policies

## **Project Time Line and Responsibilities**

The top three priorities—firewall, virus protection, and strengthening the wireless network—will receive urgent attention from our security consultant, Jeremy. The remaining tasks will be done by our own staff in order of priority.

We expect the top three priorities to be completed within a week and the remaining tasks within 30 days. Steve will be responsible for purchasing and implementing the technical changes. Kim will be responsible for all the policy and training requirements. Denise will oversee the project and be responsible for any other tasks that arise.

## **Response Planning**

In the event of a security breach, we will contact Jeremy. His company has a one-hour response policy during office hours and a four-hour response policy at all other times to deal with serious incidents, such as virus infections. In addition, Steve will monitor the server and firewall regularly to make sure that no breaches have occurred.

## **Ongoing Maintenance and Compliance**

Steve will be responsible for security on a day-to-day basis, with Denise taking overall responsibility. Steve will continue his own self-education on the topic, subscribe to

security bulletins from Microsoft and our antivirus software supplier, and liaise with Jeremy on a regular basis to monitor compliance with the new policies.

On a monthly basis, Steve will make sure that Windows and our antivirus software are updated and that the backup and restore procedures are working properly. He will also be responsible for ensuring that new computer equipment is properly configured and up-to-date.

Kim will be responsible for ensuring that new employees that join the company are fully trained in the company's security policies and procedures.

There will be a full, formal review of this plan in six months.

### ***Section 4: Resources and Budget***

The following expenditure has been approved:

#### **Software and Hardware**

- Purchase antivirus software.
- Configure Office Outlook 2003 to filter junk e-mail.
- Install a hardware firewall.
- Replace the last four desktop computers running Windows 98 with computers running Windows XP Professional with SP2.
- Purchase security locks and new nondescript laptop computer bags.
- Check into additional backup media.

#### **Professional Advice**

- Sutton and Sutton to review our rewritten staff policies
- Jeremy for advice during the creation of this plan
- Jeremy for help with implementation

#### **Internal Resources**

- Although we are not paying for our own staff directly, to be clear about the allocation of resources and the time that is available for this work, we have authorized the use of internal staff as detailed above.