

Large Animal VETERINARY Rounds™

AUGUST/SEPTEMBER 2004
Volume 4, Issue 7

AS PRESENTED IN THE ROUNDS OF THE DEPARTMENT OF LARGE ANIMAL CLINICAL SCIENCES
OF THE WESTERN COLLEGE OF VETERINARY MEDICINE, UNIVERSITY OF SASKATCHEWAN

Protecting your Veterinary Practice from Data Loss

By Brian Buydens, B.Sc., B.Ed.

Many businesses are dependent on computer systems to maintain their data, including vital financial information and product inventory. In a veterinary practice, the computer also contains confidential patient and client information. Given the dependence businesses have on computers, it is surprising to realize just how vulnerable they are to data loss. Data loss can occur from many causes (eg, lightning, fire, theft, computer equipment malfunction, hackers, or computer viruses) and can be devastating to a company or medical practice but, with common sense, it is possible to reduce the risks. Not everyone has the expertise or time to set up a secure computer system; however, knowing the options for configuring one can help you ask the right questions and make informed decisions. This issue of *Large Animal Veterinary Rounds* provides a primer on the use of computers and incorporating a system into your veterinary practice, offers advice on choosing a new system, and addresses the sources of data loss and how to prevent them.

Choosing a system

Since there are 2 main sources of computer data loss – the computer system itself and external threats – the first step is choosing a system and then deciding which configuration best suits your practice. One common configuration for larger practices has a number of “client” workstations connecting to a “server.” The server has the database, shared files, and often a network printer. Servers should be kept simple, with minimal software, because a simple system tends to be a stable system. Although factors such as price, speed, and hard drive space are important in determining the final choice, the following questions are even more important:

- What kind of reputation does the manufacturer have in assembling computer systems?
- How long does it take for replacement parts to arrive?
- After a theft, how long would it take to reassemble a fully functional computer system?
- What is the availability of replacement parts after several years of operation?
- Which parts are most likely to break? With those parts missing, can the computer system still function?
- Can the computer system handle random events such as power outages and lightning?

The W.C.V.M. Database Server – top of the line

The Western College of Veterinary Medicine (WCVM) database server, purchased in 1998, consists of a computer with redundant power supplies, a redundant array of independent drives (RAID)-5 hard disk controller, an uninterruptible power supply (UPS), and hot swappable hard drives. It can handle up to 80 simultaneous database connections over the network. In terms of speed and hard drive space, this computer system operates at a fraction of its capacity and, although it was initially expensive, it is still in service after 6 years. Therefore, the price per year is actually quite



WESTERN COLLEGE OF
VETERINARY MEDICINE



Department of Large Animal Clinical Sciences Western College of Veterinary Medicine

Jonathan M. Naylor, DVM, Diplomate ACVIM
(Editor)

Charles S. Rhodes, DVM, MSc (Dean)

David G. Wilson, DVM, Diplomate ACVS
(Acting Dept. Head)

Ken Armstrong, DVM, Professor Emeritus
Sue Ashburner, DVM

Jeremy Bailey, BVSc, Diplomate ACVS

Spence M. Barber, DVM, Diplomate ACVS

Albert D. Barth, DVM, Diplomate ACT

Frank Bristol, DVM, DACT, Professor Emeritus

Ray Butler, DVM, Professor Emeritus

John Campbell, DVM, DVSc

Claire Card, DVM, DACT

Terry D. Carruthers, DVM, PhD

Bill Cates, DVM, Professor Emeritus

Chris Clark, VetMB, MVetSc

Peter B. Fretz, DVM, Diplomate ACVS,

Professor Emeritus

Paul Greenough, DVM, Professor Emeritus

Jerry Haigh, DVM, Diplomate ACZM

Steve Manning, DVM, Diplomate ACT

Reuben J. Mapletoft, DVM, PhD

Kelly MacLellan, DVM

Colin Palmer, DVM, Diplomate ACT

Andre Palasz, MSc, PhD

Jag Patel, DVM, Diplomate ACT

Lyall Petrie, BVMS, PhD

O.M. Radostits, DVM, Diplomate ACVIM,

Professor Emeritus

Fritz J. Schumann, DVM, MVetSc

Joseph M. Stookey, PhD

Hugh G.G. Townsend, DVM, MSc

Cheryl Waldner, DVM, PhD

Murray R. Woodbury, DVM, MSc

Western College of Veterinary Medicine Department of Large Animal Clinical Sciences

52 Campus Drive

University of Saskatchewan

Saskatoon, Saskatchewan S7N 5B4

The editorial content of *Large Animal Veterinary Rounds* is determined solely by the Department of Large Animal Clinical Sciences, Western College of Veterinary Medicine



The Canadian Veterinary Medical Association recognizes the educational value of this publication and provides support to the WCVM for its distribution.

reasonable and the stability of not switching computer systems is an added bonus.

Power outages do not affect the WCVM server (although they do affect client machines). The server can run for 30 minutes on its uninterruptible power supply (UPS) while waiting for power to be restored, after which, it closes the database and shuts itself down. When power is restored, the server reboots and automatically restarts the database. The UPS also protects against lightning by buffering power fluctuations and sensing spikes in the electrical current. The server configuration is based on proven technology – not the cutting edge – allowing for a stable machine with available replacement parts that are usually delivered within a day.

The most vulnerable physical part of any computer system is the hard drive. These electromechanical devices have rapidly moving parts and often fail after 3 years of service. The WCVM server is 6-years-old, but its RAID 5 hard drive system has not yet experienced hard drive failure. There are actually 5 types of RAID hard drive configurations (6 if you count RAID 1.5, a combination of RAID 1 and RAID 5). Each number specifies a different configuration type. When buying a RAID controller, it is important to specify the number. A RAID 5 controller manages a set of hard drives and each one carries some redundant information about the other drives. Therefore, if one hard drive fails, the others have enough information to recreate the data stored on the failed drive. The disk controller can sense when a hard drive becomes defective and turns off the power to that drive; the system continues running on the remaining drives. A spare drive mounted in the computer is then automatically powered up, formatted, and re-initialized with the data of the dead drive. Meanwhile, the server keeps running and servicing requests. The drives are hot swappable, meaning that the dead drive can be removed and replaced by a functional drive without shutting down the system.

A hard drive failure severe enough to stop the server would require 3 of the drives to fail in 1 day. The first failure would trigger the replacement of the failed drive by a swappable drive. The second failure would cause a slowdown in the system as the hard drive controller reconstructs the missing data from the redundant data on the remaining hard drives. Only a third hard drive failure would bring the system down. The WCVM takes precautions against hard drive failure by replacing them after the warranties expire and before they fail.

In the case of theft or fire, the system is regularly backed up on tapes that are stored off-site. The tape drive is one that is commonly available, so a replacement can be easily obtained. Changes made to the database since the last back-up (called journal files) are copied over the network to a separate machine. Once a replacement machine is chosen, the database can be functioning again in about half-a-day.

Currently, the WCVM is implementing back-ups on removable hard drives which will enable the restoration of data in about 45 minutes.

Some general tips

Not every practice requires such an elaborate system; however, it is still possible to have a stable and reliable system. Here are some general rules of thumb for any size of system.

- The server should have only the software necessary to run the database and share files. Each addition of software increases the chance of incompatibility. If possible, software applications should not be accessed directly at the server console to limit the possibility that an application may crash the server.

- If possible, do not connect the server to the Internet since it is a major source of viral infection and hacker attack. Effective countermeasures are simply to keep the server unconnected or to use a separate computer for Internet access. The separate computer could also function as a back-up to the main computer, but should not store sensitive data. If the server must be connected to the Internet, keep the anti-virus program up-to-date and apply critical updates to the operating system.

- “Disk mirroring” is a more modest alternative to the powerful, but expensive, RAID 5 system for handling hard drive failure. Disk mirroring requires 2 hard drives. When information is recorded on one, it is simultaneously written on the other. Each drive is an exact copy of the other. Therefore, if one fails, the other contains the data. In server versions of Windows, disk mirroring is a built-in option. Although an extra hard drive adds to the total cost of the system, it greatly reduces the risk of data loss if the hard drive fails.

- An often-overlooked threat to system reliability is the operator, who may make changes to the database with unintentional consequences. One veterinary practice lost business records on its first day because an employee made a mistake while adapting to the new system. The practice was able to re-create the data based on paper copies of transactions, but lost valuable time. Training is an expensive, but important part of implementing software applications.

- A server should have a UPS. The extra cost is worth it because most database programs do not take kindly to being suddenly shut down with open files. A UPS gives a time window between power loss and computer shutdown and filters out random power fluctuations, thus reducing unexplained computer crashes and protecting expensive computer hardware.

Storing data

Off-site storage of back-up data is the sole way to protect against fire or theft. Do not back-up the programs,

Case study: A one-computer veterinary practice

- When setting up your computer system, start with a good-quality computer from a dependable company that can provide parts and service in a timely manner and attach it to a UPS. The UPS will protect the computer from sudden power-outages and offers some protection from lightning
- To avoid the risk of hard drive failure, disk mirroring is an affordable option. Get at least two USB hard drives or memory sticks for backing up data; one back-up can be stored at the office, but at least one other should be stored off-site. Alternate between the devices when backing up the system. Always use the device with the oldest data set for the next back-up.
- Decide on the software you need and install it. Store the program disks in a safe place along with product serial numbers and passwords. Once the system is configured, make as few changes as possible. Critical system updates and virus updates are necessary, and should be performed promptly. Do not add other software unless necessary. When trying out new software, find another machine, do not use your main practice computer.
- Make sure everyone in the office knows how to use the software. Train them if necessary since it can be very

expensive to re-create a mangled database system.

- If the system is connected to the Internet, make sure your computer has a firewall and an anti-spyware, as well as an antivirus program. Configure the firewall correctly, use it wisely, and it will be your friend. Run the anti-spyware program after surfing the Internet to remove any unwanted parasites. Making sure the antivirus program is up-to-date protects from all but the most recent viruses. Even if the computer is not connected to the Internet, it needs an antivirus program since floppy disks are sometimes infected and it only takes one to ruin the system.
- Make sure none of the computer accounts has a blank password. Be careful when connecting to the Internet, avoid opening email attachments unless you are sure they are safe, and monitor the computer regularly.
- Avoid accessing game sites or using “cute” screen savers that can be downloaded from the Net as these can be a source of virus infection.

No system is 100% safe, but these tips will greatly reduce your risk of data loss.

just the data. Keep the original disks for the programs because if the system crashes, they will need to be re-installed.

Traditionally, magnetic tape was the medium of choice for back-ups, but USB (universal serial bus) and Firewire (sometimes called IEEE 1394) hard drives are becoming popular. They are inexpensive, have good throughput, and most computers can read them without special hardware (especially USB drives). It is a moot point which is better. Firewire is faster than USB, but USB is better supported. Almost all Intel-based computers since Windows 2000 have USB ports. However, it is possible to purchase a hard drive with both USB and Firewire support. Some interesting USB storage options include pocket USB drives and USB memory sticks, both do not require an external power source and so are easy to move and store. Currently, memory sticks are limited to approximately 1 gigabyte, but this may be sufficient to hold business records.

Backed-up data should not be stored in the office since all will be lost if there is a fire or theft. One system is to have 2 back-up drives. Data can be backed up at the end of the day and the storage device placed either in a locked fire-proof safe or safety deposit box, or taken home. The second back-up drive is removed when the first is placed in storage and it is used for back-up the next day. Storing back-up drives or tapes at a different location gives added protection, but there is the risk of losing them during transport. Back-up drives are easy to steal and should be kept locked-up

because, if stolen, you have not only lost data, but also the confidentiality of your clients.

The Internet – User beware

As mentioned above, whenever possible, do not connect your business computer to the Internet. If the Internet is necessary (eg, for email), use a second machine. When connected to the Internet, special care is necessary to ensure your computer is not hacked, attacked, or compromised in some way. To understand attacks from the Internet, it is helpful to have a conceptual framework of how these attacks occur.

The simple diagram in Figure 1 can describe a variety of systems, but in a computer system, the “black box” is the computer. “Input” comes in many forms (eg, email, the keyboard, web browsers, floppy or removable disks etc.); “output” can be files, web documents, email, or printouts;

Figure 1: Generic feedback system diagram

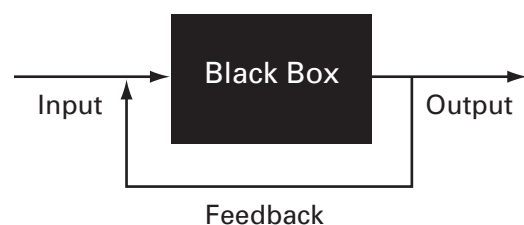


Table 1: Common computer jargon

Exploit	– a flaw in the computer software or configuration that allows a hacker access to the system
Phishing	– sending fraudulent emails to obtain confidential information
Script kiddies	– people who use hacker programs to attack machines
Trojan	– a program that the hacker installs to take control of a victim computer (in reference to the wooden horse used in the battle of Troy)

while “feedback” may come from the monitor, the printer, and how the computer is operating. Attacks over the Internet disrupt this process. It may appear that the black box (ie, the computer) is the object of the attack, but often, it is not. Attacking the black box usually requires detailed knowledge of the system. Prior to the Internet, these attacks usually came from a disgruntled former employee who had access to the system. Prudent companies protected themselves by terminating the log-in accounts of former employees. The advent of the Internet changed the nature of “black box” attacks by providing easier access to computers. However, a would-be hacker usually has minimal information about a target machine and, consequently, uses a “shotgun” approach. He chooses a popular operating system (eg, Windows) and a common software application (eg, Outlook, Acrobat Reader, or Internet Explorer) and constructs a test machine. Once the hacker finds a flaw in the software that grants access to the system, he designs a program to probe machines on the Internet and attack those with a similar vulnerability.

Although black box attacks are a big problem, Internet attacks often focus on one or more systems, eg, Ebay or bank fraud. The scam begins as an email warning that there is a problem with the user’s online access to the system. The user is advised to log-in and verify his/her username and password, there may even be a link to access a counterfeit web page. In an Ebay scam, the web page looks almost exactly like the real thing and the links actually access Ebay sites, however, the web form’s username and password fields are re-directed to a third-party website that collects the confidential information for the purposes of committing future fraud.

The best way to guard against fraud is to stop it at the source. Ebay, the banks, Microsoft, or Internet service providers do not email notices telling people to log-in to their websites and provide confidential infor-

Table 2: Compromised parts in a typical email virus

Input: An infected machine sent the email. It went through the address book on the infected machine and forged the address of the sender, based on one of the entries. It is important to realize that the “From:” address is forged. The address book furnishes both a victim list and a list of addresses as disguises.

Output: The virus payload is usually disguised as something else. For example, the attachment may be called readme.txt.exe. Some computer configurations hide the final extension so you may not see the final “exe.” This makes the virus look like a harmless text file.

Feedback: Typically, clicking on the attachment and activating the virus provides no feedback. The virus quietly installs itself and begins to attack other machines.

mation. If in doubt, make your own connection *without* using the link provided. Do not trust a link that requests confidential information since the sender and location of the link can be disguised.

Computer viruses are another means of computer system attack. Some use “exploits” (Table 1) in the operating system or browser to attempt a black box attack, but most use more pedestrian means (Table 2). The user receives an email that appears to be from a friend and there is an attachment. The user opens it and is immediately infected.

Preventing a virus is the first step. Do not open attachments unless you have verified that the sender has actually sent you an attachment. Some businesses use a secure document server to send documents; here the email only notifies that a document is on the server. This procedure is much more difficult for a would-be hacker to hijack than sending email attachments. Avoid sending attachments, but if you do, give it a descriptive file name, ie, “A recent study on mosquito fogging for reduction of West Nile virus,” which is less likely to be forged than “readme.txt.” Do not automatically open attachments, first save it to disk and then run a virus scan; however, occasionally, a virus will spread more quickly than the creation of the antidote needed to detect and remove it.

Commercialism and fraud on the Internet

The last 10 years have seen phenomenal growth in the flow of money over the Internet.

Re-directing traffic: One way that individuals and companies have tried to cash in is by re-directing traffic. When a browser cannot locate a web page, an error page is often displayed with the error number

404. This error page is actually a web page that was originally generated by either the browser or the web site. However, commercial minds realized how often these error pages were received and invented ways to capitalize on their advertising potential. There are many ways to re-direct the source of the 404 error page, most are harmless and simply expose the user to unwanted advertising, but they illustrate a point. Someone has written a program to re-direct the output of computers on the Internet, for the chief purpose of making money.

Spyware is a much more recent development. While viruses predate the Internet, spyware is an outcome of its commercialization. The 404 error page exploitation, while similar to spyware, does not seek to spy or gather information. For example, a website sometimes requests the browser to store some data, called a “cookie,” on his/her computer. This cookie provides a way to track which parts of a website the user has viewed and other websites that have been visited.

Spyware cookies make it possible to predict the computer user’s interests. With the user’s email address (often obtainable from the browser), website maintainers are able to target the user with emails (a.k.a. spam) specifically tailored to their interests. Cookies do not harm the computer, but they leave behind information that potentially interferes with the user’s privacy. It is possible to configure some browsers to refuse cookies, but this may prohibit access to some websites. Therefore, it is impossible to categorically say if cookies should be enabled or disabled.

Custom toolbars are more intrusive than cookies in the information they gather and the control they exert over the computer. Internet Explorer allows toolbars as add-ons that control how the program behaves. One such toolbar is called “Alexa,” which displays websites that relate to the one currently being viewed. When the browser clicks on one of the related websites, the choice is sent to Alexa, which then uses this information to fine-tune its data. Cookies or toolbars like Alexa typically fall under the category of “data miners,” ie, they gather data about the user and report back to a central agency that may use it for market analysis or to refine the browser’s search mechanisms.

Key-loggers gather data on the user; but they also tap into the primary source of user input, the keyboard. They record every keystroke, store the output, and send it to a central site for analysis. If you access online banking or make a purchase online with a credit card, a key-logger may capture this information and send it to a central agency. With the right software, confidential information, bank accounts, and credit cards can be accessed. Other software can also collect computer user-

names and passwords, allowing the central agency to break into other computers. Theoretically, keyloggers could also be used to blackmail. Even if a user does not use online banking or business and is certain that there is no confidential information on his/her computer, there is still one extremely useful item, his identity.

Identity theft: A classic activity in crime literature is to create the illusion that someone else is guilty. The criminal usurps the identity of the “fall-guy” and an innocent person is blamed for the crime. Computers provide a convenient means to commit “identity theft.” A virus that forges the “To” and “From” addresses stored in a com-promised machine’s address book, performs identity theft. A hacker launching an attack on a company will typically use one or more machines already compromised, preferably in different countries, to obscure the origin of the crime.

Trojan dialer: A more sinister way to hijack a web browser is a program sometimes called a “Trojan dialer.” With dial-up access, the computer dials the telephone number of the Internet service provider (ISP) and connects. The computer stores the ISP telephone number as part of its configuration. It is possible to override this configuration and replace the telephone number with a different one, effectively changing the ISP. This switch can happen while browsing and can, for example, make unwanted changes in your phone bill.

Tools to guard against Internet attack

One of the most important and easiest ways to minimize the possibility of attack is to update the operating system in a timely manner. Most “black box” attacks exploit known problems in the computer system, therefore, closing the holes can prevent an attack. In Windows 2000 and XP, the computer automatically installs and applies critical updates. Older systems require human intervention. Having an updated anti-virus program is necessary since new viruses literally spread in hours. Most antivirus software programs have a built-in mechanism for automatic updates over the Internet.

Computers that are permanently connected to the Internet are at risk of new viruses that can “infect” before the virus checker is updated. Ironically, a machine that is only occasionally connected to the Internet may be at greater risk from known viruses than one that is continually connected since it will have an out-of-date antivirus program when updates are delivered. Keeping a computer off the Internet can be a good safety ploy; however, configure the virus checker to update every few minutes and avoid reading email until the system has installed the latest updates.

A Firewall: "Firewalls" are either physical (ie, a box placed between the company's computers and the Internet that blocks certain types of Internet traffic) or implemented through software. Recent Windows operating systems have a built-in firewall (IPSec in Windows 2000 and ICF in Windows XP). However, the Microsoft firewall only blocks incoming traffic, while other firewall products (eg, Kerio or Zonealarm) monitor outgoing traffic as well. Monitoring outgoing traffic can reveal if the computer is infected with a new virus. An infected computer wants to infect others, but when the virus tries to access the Internet, the firewall will generate a warning. While not the preferred method for detecting viruses because it only detects the virus once the computer is contagious, this method is very effective in isolating viruses that are too new for the antivirus software to detect.

A firewall can effectively protect a computer that is occasionally connected to the Internet since it doesn't require frequent updating. Many IT professionals install one before connecting a computer to the Internet for the first time. It is critical to confirm that the computer does not have any accounts with blank passwords. Hackers can easily detect a blank password and take control of the machine. In my own personal experience, an unprotected computer with a freshly installed operating system can be infected or attacked in about 1 minute after being attached to the Internet. Be safe – install the firewall first, then connect to the Internet. You may want to leave setting up a firewall to an expert since they can cause subtle, unexpected side effects. Make sure to inform the IT professional if you use network file-sharing and printing since these services often break down unless the firewall is specifically configured to accommodate them.

The main sources of spyware are free programs and websites. A free screen saver may provide a soothing picture on the monitor, but it is also a continually running program that may be the bait for a Trojan. Be cautious about downloading free programs, especially on a business computer. Try out each new program while monitoring outgoing connections with a firewall. If a spyware program tries to connect to the Internet, the firewall will detect it. However, the firewall will not detect all spyware and some (eg, Kerio) will detect when a program tries to launch another program, which can be annoying with legitimate programs. Another solution is to install an anti-spyware program that will detect and remove spyware and ad-ware. Run this software on a regular basis, especially after surfing the net. Some

common programs (eg, Ad-aware) are free (although a donation is preferred).

The bottom line

Consider seeking the advice and help of an IT professional. Tell them your needs and they will help you set-up the most appropriate configuration. It is much cheaper to prevent a problem than to repair one. The extra money spent on expert advice will be well worth it.

Brian Buydens is an I.T. professional at the W.C.V.M. and is responsible for maintaining and enhancing the software for Prairie Diagnostic Services. He is the chief technical expert for the college servers and has 11 years experience with configuring servers. Brian trained at the University of Saskatchewan and received a B.Sc. with honours in mathematics and high honours in Computer Science. He also has a B.Ed.

Resources

Viruses and spam, what you need to know

http://www.sophos.com/sophos/docs/eng/comviru/virus_ben.pdf

Use the Internet Connection Firewall

(information on the Windows XP firewall)

<http://www.microsoft.com/windowsxp/using/networking/learnmore/icf.msp>

How Computer Viruses Work

<http://computer.howstuffworks.com/virus.htm>

Arrays, RAID Drives and Striping: How They Work

http://www.creativecow.net/articles/lindeboom_ron/how_raid_works/

Upcoming Meeting

4-8 December 2004

50th Annual Convention of the

American Association of Equine Practitioners

Denver, CO

Contact: AAEP

Tel.: 859 233-0147 Fax: 859 233-1968

Website: www.aaep.org

Do you have a review article suitable for large animal practitioners? Please contact the editor by E-mail, Jon.Naylor@usask.ca for publication and remuneration details.

Change of address notices and requests for subscriptions to *Large Animal Veterinary Rounds* are to be sent by mail to P.O. Box 310, Station H, Montreal, Quebec H3G 2K8 or by fax to (514) 932-5114 or by e-mail to info@snellmedical.com. Please reference *Large Animal Veterinary Rounds* in your correspondence. Undeliverable copies are to be sent to the address above. Publications Post #40032303

This publication is made possible by an educational grant from

Schering-Plough Animal Health

© 2004 Department of Large Animal Clinical Sciences, Western College of Veterinary Medicine, which is solely responsible for the contents. The opinions expressed in this publication do not necessarily reflect those of the publisher or sponsor, but rather are those of the authoring institution based on the available scientific literature. Publisher: SNELL Medical Communication Inc. in cooperation with the Department of Large Animal Clinical Sciences, Western College of Veterinary Medicine. TM*Large Animal Veterinary Rounds* is a Trade Mark of SNELL Medical Communication Inc. All rights reserved. SNELL Medical Communication Inc. is committed to the development of superior Continuing Medical Education. The administration of any therapies discussed or referred to in *Large Animal Veterinary Rounds* should always be consistent with the recognized prescribing information in Canada.