

System security is important to your dealership

The only computer system that is truly secure from malicious electronic attack is one that is turned off! And even when turned off, there are physical loss or damage considerations that must be taken into account to manage the security risk. A dealership must weigh the costs of protecting vital, business-critical information against the loss of convenience that increased security measures entail. For every dealership, there is a balance that lies somewhere between a totally open and available system and one that is completely locked down and "secure".

The knowledge of a dealership's staff and the information that supports and records their activities are business assets that cannot easily be replaced if lost. It is often the case, however, that these assets do not receive the same consideration that physical assets are given when an insurance and security plan is developed.

IT managers and security administrators need to continually ensure that they are taking "reasonable" measures to protect business assets as the level of threat to their systems and the value of their electronic information increases. Security managers must also consider the cost of unauthorized access to and the manipulation of data, stolen customer information, and the impact of the exposure to the Internet community of private financial and credit information.

This issue of *Password* highlights some of the products and services that IBM and PFW provide to our customers to assist them with implementation of a security plan that is appropriate to their dealership's specific needs. We also outline several of the threats to dealership staff productivity that constantly drain energy away from their primary purpose—to serve your customers.

Security features are built into PFW eServices

PFW's eServices allows you to provide customer care beyond regular business hours. Known as a self-service application, eServices allows customers to look after their own account – on their own time. Using an Internet connection, your customers can easily view details from outstanding balances, parts and service quotes, to scheduling and ordering parts from your dealership.

With eServices your data is secure, using the Internet connection and PFW's technology without the fear that your customers' data is available to intruders. PFW's eServices security features prevent hackers, even the competition, from reading your customers' data.

The sign-in screen is the first security feature built into eServices. For your customer to have access to eServices, they are required to have a username and password which are linked to a specific customer account. Only one customer account number can be assigned for each username and password, so your dealership can be confident that your customer has access to only their account information.

Dealerships can be assured that PFW has given security issues priority while developing our eServices software. Your dealership has the option to allow customers to access the modules pertaining to account, equipment, purchasing, purchase history, quotes and messages/specials. In addition, purchase order requests, display availability, display prices, display discount messages/specials, display cross reference parts, generate picpak, issue parts and the ability to order service agreement parts are also under the control of the dealership.

*According to Sophos Anti-Virus,
the number of new viruses
will continue to increase.
In 2001, there were an average of
700 new viruses created each month.*

IN THIS ISSUE

eServices continued <i>Security features</i>	pg. 2	Wireless LAN Security <i>Protection against "war driving"</i>	pg. 5
PFW's Bi-Annual Conference <i>Coming in March 2003</i>	pg. 2	Upcoming PFW Workshop <i>Dec. 11-13, 2002, London, ON</i>	pg. 6
The iSeries Approach <i>iSeries security functions</i>	pg. 3	Virus & Email hoaxes <i>How to recognize a hoax</i>	pg. 7
Keeping your Info Secure <i>Basic checklist for security</i>	pg. 3	PFW customer list grows <i>Welcoming new dealerships</i>	pg. 8
Internet Firewall Solutions <i>How can PFW help?</i>	pg. 4	PFW helps farmers <i>PFW makes charity donation</i>	pg. 8

Continued on page 2

eServices...Continued from page 1

With the equipment module, your customers can view recommended service agreements, but as a security feature, your dealership has the authority to stop internal service agreement programs from being seen. You can also control whether the customer can order from recommended parts lists.

Customers who are allowed to modify their customer profile can make changes such as name, address and telephone number. Each user represents a contact on the customer's account, which does not affect the master profile information. Every time the customer makes a change, an email is sent to the dealership showing the changes before and changes after.

For complete security, all customer activity can be logged. You can easily discover which customers are accessing which screens and when. This information can also be helpful for making changes to eServices. For example, if you notice no one is accessing the eSales module, you can decide if eSales needs promoting.

Utilizing the strength of the iSeries, eServices is a powerful application that will help extend your customer care program one step further and keep your customers' data safe. The iSeries 400 has very strong system security characteristics and flexibility that allow you to set up your system security to meet your specific requirements.

If you would like more details about PFW's eServices, contact Suzanne Kantor or Trish Rogers at 519-474-3700.

Above: The user, Robert, has access to all eServices modules. Robert does not have authority to generate picpak, issue parts and order SAM parts. Branch and customer information and shipping information is also displayed.

More details are coming...

PFW Dealership Management Conference – March, 2003



While the specific dates for next year's Dealership Management Conference are not yet firm, preparations and site selection are currently underway. Watch PFW's web site (www.pfw.com), your e-mail and the next edition of the PFW *Password* for further details regarding this exciting event!

PFW looks forward to your participation at the PFW Dealership Management Conference in March, 2003!



PFW Password is produced by PFW Systems Corporation, for our system users and others, and is distributed free of charge. Any comments or submissions are welcome, and should be addressed to the editor:

c/o PFW Systems Corporation
 850 Medway Park Court
 London, Ontario, Canada
 N6G 5C6
 Phone: (519) 474-3300
 Fax: (519) 474-3949 **OR E-mail your suggestions to grigg@pfw.com**

The iSeries approach to security

Like so many other functions on the iSeries 400, security was built in from “day one” as an integral element of the original system design architecture. IBM’s security experience with large, multi-user mainframes gave the original OS/400 developers a significant advantage over other operating systems that were first developed for desktop systems and then extended and enhanced for Intel-based servers.

Many PC-based viruses are introduced on Intel-based servers or desktops as attachments to documents that, when detached or activated, are converted into programs that can then execute harmful command sequences. By contrast, the hardware and software architecture of the iSeries 400 (formerly AS/400) offers a much higher level of security to its users. Every stored object, whether program or data, is validated by OS/400’s security component and by the AS/400’s System Licensed Internal Codes authority component. This multi-layered object authority validation prevents objects being transformed from innocuous data to malicious virus or worm.

No iSeries 400 has ever been reported to have been infected by a virus! Although the iSeries 400 and OS/400 are thought to be immune from a direct virus attack, the system can still serve as a host for a virus that will infect other Intel-based servers and desktops in your network. This can happen when the iSeries 400 is used to receive and store e-mail messages (e.g., with Lotus Notes) or as a storage facility for PC files (e.g., with Client Access). To prevent this from happening, a number of vendors offer anti-virus scanning software for the iSeries 400 to protect against further distribution of these stored viruses.

The iSeries 400 was designed for businesses that require levels of security ranging from nothing at all to full government-certifiable (C2) security. In



addition to the five basic system security levels, the security administrator must also define user security through the configuration of individual user and group profiles.

Every user of the iSeries 400 must have an assigned user profile. A user profile defines the level of system access a user is permitted as well as the functions each user can perform. A user profile also determines the files and programs that each user owns and has access to. Users gain access to the iSeries through a password system that itself can be configured in a number of ways to ensure uniqueness, length, expiration, and the level of system tolerance for failed signon attempts.

The OS/400 operating system can be configured as one of the most secure operating environments for business use. The secret formula for providing your iSeries 400 with adequate security is understanding and using the many different security features that are provided within OS/400. It remains the responsibility of the system administrator to make it so.

Keeping Your Information Secure and your Network Healthy

1. Back up your system regularly! Your dealership’s information is a critical business asset. Ensure that the backups are complete. Take a backup copy off-site on a regular basis – at least weekly. This is still the most important security measure you can take!
2. Maintain strict control over all system passwords. In the iSeries environment, QSECOFR is not the only system password that must be protected. Do not leave any iSeries system password at the default or initial setting.
3. Set the OS/400 security level to 40. This is the lowest security level recommended by PFW.
4. Assign each user a unique ID with a password that regularly expires. This tends to “weed out” old user IDs and invalidates passwords that may have been given out for “one-time” use. (You can set criteria on the iSeries for passwords that are increasingly secure.)
5. Educate your users to the importance of network security. Grant each user the minimum level of authority that they

Continued on page 6

Internet Firewall Solutions: How can PFW help?

It's safe to say that by this point in time almost everyone involved with a business Internet environment has at least a passing familiarity with the term 'firewall'. Security is the most important issue concerning the Internet today and how well, or poorly, your business implements an Internet security solution can have wide-ranging effects well beyond your internal network. It may be hard to believe that a gap in your Internet security policy could have repercussions for Internet users elsewhere in the country or around the world, but it's no joke.



InstaGate EX2

For example, long past are the days where computer viruses, once activated, simply affected your PC, needing your help to spread from one computer to another by diskette or copying a file. Now, "blended threat" viruses such as the Code Red virus are designed to exploit vulnerabilities in operating systems and commonly-used programs and use those vulnerabilities to spread the virus infection to other potential victims on the Internet. Once a system has been infected, it may start sending out thousands of probes to other Internet hosts, looking for more vulnerable systems to pass the virus to.

Let's say your system becomes infected with one of these active viruses. It searches the Internet for new victim systems and finds five, infecting those. Those five then also begin searching the Internet for further machines to infect. Each finds an additional five, and then those begin searching – our original single infected system has now created 30 newly-affected machines, in a span of

what may only be a few minutes. You can see how it could take just one lapse in security to create a cascading chain of events affecting systems far and wide.

This may all sound somewhat frightening – and it should be. A lax Internet security policy can not only cost your business time and money but can very easily spread the pain around. Fortunately, the good news is that it's relatively easy to protect yourself against Internet risks, once you're aware of your options and how to implement them.

A firewall, sometimes also called an Internet security appliance, is the best all-around solution you can buy to make your network more secure. Because your internal network connects to the Internet at a single point (your Internet router), it's easy for a firewall, installed between the router and your internal network connections, to examine all network traffic passing between your network and the Internet. The firewall will examine each bit of data passing through it and decide whether or not that data should be allowed to continue to its destination – all based on rules configured into the firewall, which can be customized for your needs.

In addition, most firewalls also support additional security features that can add

extra layers of protection to your network. For example, anti-virus support can scan incoming and outgoing e-mail messages and detect and remove viruses before they even reach your users' inboxes; secure VPN (virtual private networking) support allows authenticated remote users to gain access to your network from another location on the Internet in a secure fashion; and security logging support allows the network administrator to monitor Internet traffic and adjust firewall settings as necessary.

To provide a firewall solution to our customers, PFW has partnered with eSoft, Inc., manufacturer of the InstaGate EX2 and InstaGate PRO security appliances. The InstaGate offers firewall security and remote VPN access for a network of any size, and is customizable with many add-on packages to meet a diverse range of needs. Anti-virus, web site and application filtering, as well as dial-up modem support and full web server and DNS server support are a few of the options available for the InstaGate. Set-up is quick and easy, and the device can be providing firewall security, as well as any additional features you may have chosen for your network, in a very short time.

Your Internet security policy will naturally vary depending on the number of users at your location, the type of servers you run and the kinds of services you provide to the Internet in general. However, what does not vary is the importance of having such a policy and ensuring that your network is as secure as possible. All users of the Internet, in addition to your local users, will benefit.

For more information on the InstaGate security appliance from eSoft, or to discuss how PFW can help you with your Internet security requirements, please contact:

Tim Whitley at 519-474-3700 for technical details; or
James Brown or Brian Lewis at 519-474-3300 for pricing details.

For all other inquiries, please contact Debbie Naujokaitis at 519-474-3300 ext. 230.

Wireless LAN Security: How to protect against “war driving”

Wireless networks have received a lot of attention from hackers looking for ways to exploit the newly-formed networks.

Wireless networks developed around the Wi-Fi (802.11b) standard become more popular with each passing year. The widespread adoption of wireless networks is mainly due to the mobile connectivity they provide, as well as their easy set-up. As a result of the rapid adoption rate, wireless networks have received a lot of attention from hackers looking for ways to exploit the newly-formed networks. In a practice known in the hacker community as “war driving”, a hacker equipped with a notebook PC and wireless card will drive around near office buildings looking to find an open wireless network. Once an open wireless network has been discovered, the hacker may use it purely for Internet access, attack machines connected to it, or launch attacks on other computer systems through it. To assist in preventing hackers from gaining access to your company’s network through your wireless investment, there are four main security measures you can implement.

Some of the most basic features of your wireless network are enabled by the manufacturer to make it easy to get your wireless network working right out of the box. Unfortunately, without any work on the part of the hacker, it is often these features that leave your network open to attack. If, during the set-up of your wireless network, you plugged in your access point and installed your client cards without any further configuration, you are at risk of a hacker attack. Risk can be quickly lowered, however, by making one simple configuration change. In your access point’s configuration, turn off “broadcast network name”, and your risk

will be lowered. If broadcasting is enabled, and you do not have encryption turned on, anyone with a PC and a wireless card will be able to connect to your wireless network. Every wireless network has a special name that is used to identify it. If “broadcast network name” is turned on, the access point will inform every client in range what the name of the network is, allowing them to connect. If broadcast is turned off, only clients that have been configured with the network name will be able to connect. Think of the network name as a secret pass code: only clients that know the code will be able to join.

Another common way to help prevent hackers from connecting to your wireless network is by enabling WEP (Wired Equivalent Privacy). WEP encrypts the data sent between the client and the access point. To set-up WEP, a special code consisting of letters and numbers is typed into the access point’s configuration. Each client that requires access to the wireless network also needs to have the key typed into the adapter’s configuration. When WEP is enabled, data being sent from the access point to the client computer is encrypted using the key installed in the access point, and decrypted using the key installed in the client computer. Unfortunately, WEP is not 100% secure, but it does add an additional level of security.

There are advanced security features that not all wireless networks support, but if support exists, they can lower your risk of hacker attacks. The most common feature is MAC (medium access control) filtering. Every wireless client card has a MAC

address consisting of a series of letters and numbers. The address is designed to be a unique identifier, and no two cards should have the same one. Certain access points can be configured to either allow access to a specific MAC address, or disallow access to a specific MAC address. Adjusting your access point to only allow recognized client adapters to connect will add additional security to your network, but should not be considered a method that is hacker-proof.

The most effective way to prevent hackers from connecting to your wireless network is to prevent the wireless signal from leaking outside of your building. Hackers need to be within working range of your wireless network to attempt to connect. If the wireless network is limited to the confines of your building it effectively prevents the hacker from making a connection. Strategic placement of your wireless access points, as well as adjusting their power levels, can ensure the wireless network is mostly contained within your building.

Hackers that spend their time “war driving” are a reality, and one which is not going to disappear any time soon. As long as there are unsecured wireless networks that are easy to gain access to, hackers will continue to exploit them. Your wireless network will always be at some level of risk, but that risk can be lowered by taking advanced actions. Turn off “broadcast network name”, enable WEP where possible, disallow MAC addresses other than your own, and try to contain your wireless signal to the confines of your building. Following these recommendations will make your wireless network a less appealing target for “war drivers”.

For more information, contact Joshua Van Buskirk, Mobility by Design, at 519-474-0295 or vanbuskirk@pfw.com. You can visit Mobility by Design’s web site at www.mobilitybydesign.com.

Keeping your information...Continued from page 3

require to perform their assigned tasks – no more. The majority of the security breaches you are likely to experience will be from users inside the organization. Many security breaches result from advanced stages of curiosity. An accidentally-deleted file can be just as devastating as one that was deleted on purpose.

6. Desktop PC users should each run an up-to-date copy of virus protection. Users should understand that hundreds of new viruses are created weekly. Ideally, virus protection should be managed centrally to ensure efficient and current level updates.

7. When connected to the Internet use a firewall, as a minimum level of protection, to block unwanted incoming and outgoing traffic. Your ISP can provide this protection, or you can use a network security appliance, such as the Instagate, to provide protection from network intrusion. A network appliance can be

configured for firewall, anti-virus scanning, and application filtering.

8. Application filtering will allow you to determine if your network bandwidth is being used productively. There are a number of programs and activities that generate significant, but non-productive, traffic on your network (e.g., MP3 file sharing, multimedia audio or video streaming sites, webcams or active weather radar displays). Some of these should be turned off completely or restricted to non-critical, after-business hours.

9. Turn off all services that are not necessary on your servers (e.g., FTP, telnet, web serving, etc.)

10. Use VPN (Virtual Private Networking) connections for remote users and sites to encrypt the data at one end of the connection and decrypt it at the other end. This provides a “virtual tunnel” between the two sites which is not visible or accessible at any point in between.

IBM iSeries 400 Upgrades

PFW System users who recently upgraded their IBM iSeries 400:

Agland Corporation - Lloydminster, AB

Bobcat of Lansing - Lansing, MI

Coneco Equipment - Edmonton, AB

Farm World - Kinistino, SK

Martin Equipment - Edmonton, AB

Huron Tractor - Exeter, ON

Les Equipements Ligue - Ste. Rosalie, PQ

Lyons Sawmill & Equipment - Little Valley, NY

PFW Workshop Advanced Service and Equipment Management | November 13-15, 2002, London, Ontario

Proposed Workshop Sessions Include:

Service Management

- Service Agreement Management | *Creation and Maintenance of Preventative Maintenance Contracts*
- Management Central | *Track Work in Process and Schedule Technicians and Shop Bays*
- Barcoding of Work Orders for Labor Entry
- Remote Entry of Labor Hours for on-the-road technicians
- Utilizing Flatrates and Service Pricing Guides
- Service Management Reporting

Equipment

- Equipment Invoicing Capabilities for Salesmen and Accounting Department
- Mobile Salesman | *How it can Help your Sales Staff*
- Traffic System | *How it Helps Manage your Inventory*
- Wireless Applications | *Equipment Tracking*
- eSales Capability within eServices
- Equipment Reporting
- Utilizing Management Central for Equipment Management

Workshop Details

Workshop: Advanced Service and Equipment Management
 Date: November 13-15, 2002
 Location: Spencer Hall, London, Ontario
 Price:* \$575.00 USD (3-day session)
 \$775.00 CDN (3-day session)

*Prices are subject to change and do not include accommodations

Who Should Attend?

- Equipment Managers
- Service Managers
- System Administrators

Space is limited to 50 attendees. Registration is on a first-come-first-served basis.

Contact Laurie Brown at 519-474-3300 ext. 237 or email lbrown@pfw.com to reserve your place.

True or False: virus and e-mail hoaxes

In 1989, the US Department of Energy created a group called the Computer Incident Advisory Capability, whose objective it is to research and “debunk” both virus and e-mail hoaxes as part of their usual security initiatives. Worldwide, many other organizations exist that dedicate a great deal of resources to the same objective. Why? Because with the number of Internet users increasing every year and the amount of information growing exponentially, it has become a difficult, full-time mission to separate the real threats from the phony ones. These organizations are working to fight the overload of the “Internet misinformation” that costs individuals and organizations billions of dollars each year, uses valuable time and resources and even compromises network security.

This article is intended to provide you with some information on virus and e-mail hoaxes – including tips on how to recognize a hoax, how to be a “hoax-buster,” where to go to get information on real and phony viruses and advice for taking action against hoaxes that you can use at your dealership today.

Recognizing virus and e-mail hoaxes

Usually forwarded via an e-mail message, virus hoaxes may claim, in impressive-sounding, pseudo-technical language, that a particular virus is extremely dangerous and that you must tell everyone you know about the threat. The hoax may even make the claim that the virus warning was issued, or confirmed by, a well-known company or individual. An e-mail hoax (sometimes referred to as a “chain letter”) can contain pleas for sympathy, describe a situation where you may be entitled to money from a large corporation, warn you of government conspiracy or inform you of health risks that “you’re not supposed to know about.” Even though they are somewhat different in composition (virus threats contain technical-sounding language and list a “credible” source and e-mail hoaxes often contain a hook, a

threat and a call to action), they usually contain common characteristics.

Virus and e-mail hoaxes often:

1. Are geared more towards persuading than informing.
2. Contain the telltale phrase “Forward this to everyone you know.”
3. Make statements like “This is not a hoax” or “This is not a joke” – usually indicating the opposite.
4. Make frequent use of empathetic language and UPPERCASE LETTERS, contain bad spelling and grammar and multiple exclamation points!!!!
5. Typically do not refer to a third party that can validate the claim or offer links to web sites with corroborating information (conversely, virus hoaxes may make reference to organizations that don’t exist).
6. Purport to give you extremely important information you’ve never heard of before or received elsewhere from legitimate sources (e.g., the newspaper, TV news or in industry magazines).
7. Make wild claims that violate your common sense.

Do your homework and be a hoax-buster!

If you receive an e-mail that exhibits any of the characteristics listed above, or has dubious origins, your safest bet is to remain cautious before forwarding it on to anyone else or opening any of the attached files. Even if the e-mail is from someone you know, it’s always worth checking it out first – in the end, you’ll save yourself the embarrassment of forwarding “false” claims to other people (and continuing the spread of misinformation) – and you’ll be protecting yourself and your computer from real virus attacks. Having said this, the best advice we can offer is still this: Educate yourself – and if in doubt, delete, delete, delete!

The following are excellent “hoax-busting” sites that will help you stop the spread of Internet misinformation:

- www.snopes.com
- www.vmyths.com
- www.truthorfiction.com
- www.sophos.com
- www.ciac.org/ciac/

For general virus information, information on current virus threats and removal tools, make it a habit to visit the following sites on a regular basis:

- securityresponse.symantec.com
- www.mcafee.com
- www.ciac.org/ciac/

For a copy of the Winter, 2001 Password article on computer viruses (Computer Viruses: How to Protect Yourself), contact the editor at grigg@pfw.com, or view the article online at: <http://www.pfw.com/news/articles/archives/viruses.htm>.

Consider the costs

While the threat to individual users may seem minimal, organizations and businesses can suffer when virus and e-mail hoaxes infiltrate the company. Consider the time it takes for one employee to read a hoax message and then pass it on, and then consider the load on the server as that message relays to ten other people. Multiply that by 20 employees and it’s easy to see how time and resource costs can skyrocket.

Plan for action

So what can you do at your dealership to stop virus and e-mail hoaxes in their tracks? Familiarize yourself with the best information sources on the Internet and share your research with the uninformed. Develop a policy to forbid your employees from sending chain letter e-mails to other employees (or account-holders on your system), or ask them to send all questionable e-mails to an appointed person who has the responsibility to investigate the validity of the e-mail’s information. Teach your employees to “think before you forward,” and the meaning of “if in doubt, check it out.”

PFW customer list continues to grow

PFW is pleased to welcome the following dealerships to our growing list of customers.

A former DIS user, **Anderson's Sales**, purchased Cavalier Equipment (a PFW customer) earlier this year, and is committed to using the PFW Dealership Management System. Located in Cavalier, North Dakota, Anderson's Sales is a provider of new and used John Deere equipment.



Based in Oklahoma and North Central Texas, **CL Boyd Co.**, a former ADP user, is your source for new and used John Deere, used Caterpillar, Case, Komatsu and other construction equipment.

With locations in Pine Bush, New York, Wappingers Fall, New York and Newington, Connecticut, **Pine Bush Equipment** serves 10 counties in Southern New York. This former NDS user is a provider for Case, Komatsu and Kubota.



Robert's Farm Equipment joined PFW in July 2002. Located in Chesley, Ontario, some of the manufacturing lines they carry are New Holland, Suzuki, Woods and Ford.

We want to know

Let us know if you would like to receive the Client Services Update and/or the Development Details by email or continue to receive these with the monthly statements. Please send this sheet back to the attention of Jennifer Grigg: Fax #: 519-474-3949; e-mail: grigg@pfw.com.

- Yes, I would like to receive the Client Services Update & Development Details via email
- Please continue to include them with my statement

Company Name: _____

Customer Name: _____

e-mail address: _____

PFW helps farmers in need

PFW employees recently made a cash donation to Hay West. The Hay West campaign was started to aid farmers in western Canada – Alberta and Saskatchewan – with the drought of 2002. Feeling the effects of the drought, farmers are struggling to feed their livestock with the little feed they have.

“The dry summer weather on the Prairies has left hay in short supply and the small amount available is being sold at high prices,” said Nikki Smith of the Saskatchewan Cattle Feeders Association. “Hay prices run from \$80 - \$180 a bale and the freight cost is double or triple that amount.”

Farmers and businesses from Ontario, Quebec and the eastern provinces have donated money and hay. CP Rail, CN Rail and Ottawa Central Railway have donated over 100 rail cars to transport the hay for free. The federal government has donated \$250,000 to help with the hay's fumigation and the cost to load the hay.

Currently there is a waiting list of 10,000 farmers who are in desperate need of hay. Many farmers are considering selling, or have sold, entire herds of cattle because they can no longer feed them.

For more information about Hay West or how you can make a donation, please visit www.haywest.com.

This article is from the CBC News web page. For more details, visit www.cbc.ca/news/features/hay_west.html.



850 Medway Park Court
 London, Ontario
 Canada N6G 5C6
 Telephone: (519) 474-3300
 Fax: (519) 474-3949
www.pfw.com

The **PFW Dealership Management System** is “designed for dealers by dealers.” Incorporated in 1980, PFW offers years of experience developing software for equipment dealerships of all types and sizes. It's ideal for single or multi-store equipment dealers. The PFW System has been developed from the dealership's perspective. Ongoing enhancements grow with today's customer and market needs.

Not only will we provide on-site installation and training, we also have friendly, experienced customer phone support to accommodate after-hours emergency services. Regional training seminars ensure the exchange of ideas and information among PFW users. With hundreds of installed sites across North America, the PFW Dealership Management System is proven to be a reliable, stable, cost-efficient system. There's no need to look any further for your management system – it's the Ultimate Dealership Management System ... period.