Arthur J. Gallagher & Co.

Data Security Starts With You

Nearly all companies now rely heavily on electronic information. Private, sensitive information is a vital asset that must be protected by you, its custodian. In fact, you have a legal obligation to protect that data and failure to do so can have a profoundly expensive impact on your business under current Data Protection legislation.

IS THE PRIVATE INFORMATION ABOUT YOUR COMPANY, YOUR STORE, YOUR EMPLOYEES OR YOUR CUSTOMERS SAFE?

Chances are that you store this confidential information — such as credit card numbers, names, addresses and social security numbers — electronically on a computer or you transmit it electronically to your business partners.

What would you do if this data was stolen?

Do your best to prevent that from happening by practicing safety when it comes to your online, electronic world. For both customer and employee electronic data and storage, employ these best practices to do your part:

Strong passwords

Avoid dictionary words and names. Mix letters, numbers and punctuation characters in upper- and lower-cases. Eight characters or more will be exponentially harder to crack. Whatever the password, change it every three months.

Updated firewalls

Firewalls act as a gate protecting your electronic data. It is a wall that can stop a cyber-theft and it blocks and monitors any traffic that wants to come in and go out. Be sure that it is configured properly and that it is kept up-to-date. Seek outside assistance if needed to insure that you have an impenetrable firewall in place.

Two-factor authentication

When you type in a password, your system may require a second piece of information to confirm your identity. It might be a personal tidbit, like your birthplace or identification of a key image. The safest systems text a one-time code to your cellphone.

Data Security Starts With You (continued)

Encryption

Look for terminals that encode data the moment a card is swiped. With this in place, the data becomes worthless to a criminal hacker if they were able to access the system.

Segmentation

Keep your networks separate — be sure the one for your credit card readers cannot communicate to the one employees use to check e-mail. Offer free public Wi-Fi at your location? Put that on a separate network as well.

Disable remote administration

Remote administration lets your management team work from a remote location but could act as a point of entry for a cyber criminal. Like turning off a light when you leave a room, turn this feature off when it's not in use.

Check your card machines periodically

Many manufacturers stick on seals that will be broken if equipment is tampered with. It's also a good practice to photograph a terminal when it's first installed, so that you can look later for any unauthorized changes.

Following some basic safety precautions and employing best practices such as these will reduce the likelihood that your operations will be affected by cyber crime. Be diligent. Be aware. Be proactive.

Should you have any questions or need further assistance, please visit our website, send an email or call us.

Arthur J. Gallagher & Co.

McDonald's Risk Management Team
PO Box 260700
Tampa, FL 33685-0700

800.869.8402
bsd.McDRiskManagement@ajg.com

www.ajg.com/McDonalds

14BSD26672A