Risk Management Considerations For Employee Passwords

Cyber risks are a major issue for organizations today. Sensitive information is available electronically and people have the sophisticated technology and talent to take it without permission. One way to protect important information is to develop and enforce a strict employee password protection policy. A strong policy can reduce vulnerability to hackers, but everyone must do their part for it to be successful.

Risk Management Considerations

1. Ensure that default or start-up passwords are changed immediately.
2. Passwords can't include any part of the first or last name.
3. Passwords should not contain any information about the organization.
4. Passwords should be a mix of both upper and lower case letters, as well as numbers and unique characters (such as " ~ ", " ^ ", or " * ").
5. Passwords should be at least 8 characters in length.
6. Keep passwords safe. This means never sharing them, writing them down or leaving them in a public place (under a keyboard, for example).
7. Passwords should be changed every 30 days, and the same password should never be repeated.
8. Remove unused user accounts (such as past employees or summer students) immediately.
9. Computers should be in a locked mode when not in use.
10. Restrict who an "Out of Office" message is sent to. If it's sent to everyone emailing in, a hacker could learn of a specific window of time in which to hack into the system.
11. Do not automatically save passwords on favourite websites.
12. Install an automatic lockout system if an incorrect password is entered more than three times. Email the user to let them know if unsuccessful login attempts occur. This will raise a red flag.
13. All computers should be shut off at the end of the day.
14. Password protection policies should have controls in place to ensure that security standards are met.

Instituting a thorough and non-negotiable password policy is one of the best ways to protect information from security breaches. Remember, if a password can easily be remembered, chances are hackers will have no problem cracking into the system.