PRENTICE YATES & CLARK
CHARTERED ACCOUNTANTS

info@pyc.net

the newsletter of Prentice Yates & Clark

Winter 2013

15 Toronto Street
Suite 700
Toronto, Canada
M5C 2E3

(416) 366-9256
1 (800) 265-7818
Fax: (416) 366-9171
info@pyc.net

In This Issue

Age and the Workplace

Owner-managers need to plan for an aging workforce.

No wonder owner-managers have been noticing an increase in gray hair among their employees. According to the 2011 National Household Survey by Statistics Canada, 18.7% of the workers in the 18-million-strong Canadian workforce are 55 years of age or older. This is up from 15.5% in 2006 and 11.7% in 2001 of a slightly smaller workforce. By 2021, about 25% of the workforce is projected to be 55 years of age or older.

This trend is in place because the Baby Boomers (i.e., those born between 1946 and 1965) are aging. In 2011, the oldest Boomers turned 65; by the time all 9.6 million persons in that age group will have turned 65 by 2031, the proportion of seniors in the population could reach 23% from 15% in 2011.

Retirement May Be Out of Reach

However, retirement is becoming problematical for many of these workers. Of the 18 million people in the workforce, only about six million, or one third, are members of registered pension plans. Of these, only 48% are members of private-sector plans. Participation in private-sector pension plans has, in fact, been declining steadily since the early 1980s when membership was about 60%. Compounding the problem is the increasing unwillingness of employers to commit themselves to any kind of pension plan, especially defined-benefit plans. In addition, only about 24% of all tax filers contribute to Registered Retirement Savings Plans and, when they do, the amount is only around $2,800 per year or about 12% of the current maximum eligible amount.

If you put together the low participation rates in company pension plans and low savings rates in RRSPs, then add the fact that household debt is now at 163% of disposable income, it is easy to see that retirement without at least some earned income is going to be out of reach for many in the Boomer generation.

Owner-Managers Need to Adjust

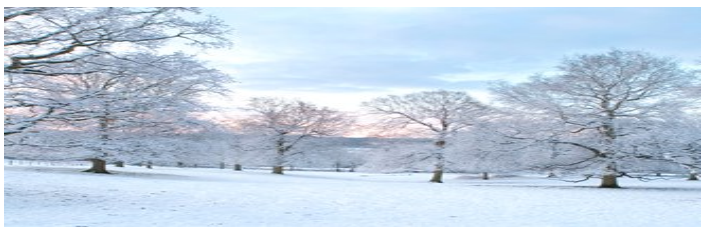
These changes in demographics and retirement savings are putting owner-managers in a difficult position. On the one hand, they know that older, long-time employees may not want or be able to retire, but at the same time they recognize the future depends on hiring younger employees. Nevertheless, by embracing the realities of age-related differences, an organization should be able to continue to draw on the experience of the older workers and the energy and new skills of the younger ones while maintaining harmony and productivity within the workplace.

▶

Holiday Donations

In lieu of seasonal gifts to individual clients, Prentice Yates & Clark made donations to the following charities:

Homeward Family Shelter
St. Clare's Multifaith
St. Hilda's Towers Foundation
Society of St. Vincent de Paul



Owner-managers will have to learn to understand the needs of older workers.

Physical Considerations

Owner-managers should take into consideration the natural aging processes when developing health and safety policies. Constructing or retrofitting the workplace with age-friendly tools may be beneficial to the business because it could reduce downtime of essential employees and the associated costs of injuries and/or Workplace Safety Insurance Board (WSIB) claims. Minor changes that can make a positive impact on employee morale:

- larger display screens and better speakers for smart phones or other communication devices
- ergonomically designed chairs and seats
- better lighting to ensure improved visibility and reduce eye strain
- limited night travel for older employees
- better designed lifting equipment
- clear markings on items in excess of a standard "safe lifting weight"
- easy-to-hold tools that increase grip without more hand power
- lighter power tools with variable power shifts to reduce sudden torque impact.

Social Considerations

Reassure older employees that you respect their experience and abilities and that they are still making a valuable contribution to the success of your business. This can be accomplished by a few simple changes:

Offer more flexible work schedules.
Reduce overtime and reschedule shifts to allow longer rest time.
Train the older worker to be a coach or mentor.
Continue professional development of individual older employees to bring out latent competencies. For example, an experienced painter might refocus as an estimator.
Revamp office, washroom, and work areas to ensure better functionality and accessibility with small enhancements such as levered handles on taps, graduated ramps and better air flow.
Address any age-related bias head on with in-house presentations that look at not only the legal implications of age discrimination, but also the similarity of needs, concerns, and desires of employees regardless of age.

Older Workers Are Here to Stay

Older workers are going to be a part of the working world for a long, long time. With a little effort and minimum expense you can continue to benefit from their experience by a bit of rethinking of workloads and scheduling. Over the next 20 years as the Boomers retire, you will need to pay special attention to your management strategies to ensure a seamless transition between the generations of workers in your business. Providing assurances to older workers that their well-being is in the forefront of your planning will ensure the continued success of the company. ♦

Password Security 2.0: Beyond the Password

Security technology is becoming more sophisticated but examine your options carefully before you upgrade.

With the release of the latest Apple iPhone – the 5s – a new security feature is now available, and the reviewers are all abuzz about this more convenient variant on privacy and data protection. But is all the hype really warranted?

There have been many great innovations and improvements in technology security and authentication over the years. Each type has its benefits and drawbacks. So, with all of these options, which is the best for your personal and business data? The basic forms of data security fall within one of three main categories: biometric, possession, and knowledge factors.

Biometric Factors

Biometrics (i.e., what the user is) are the unique physical traits of the user that can be measured and compared, such as a voiceprint, iris scan or, most commonly used in everyday technology, a fingerprint. While only you possess the originals, biometric factors are nevertheless vulnerable to being copied.

Fingerprint scanners - While not a new innovation, Apple's 'Touch ID' sensor on the iPhone 5s has once again brought mainstream attention to using fingerprints as a convenient way to let your phone know that you're, well, you. Early reviews suggest that the new sensor is convenient and effective and a considerable improvement over the older-style "swipe" sensors more common on business laptops. However, as with all biometric factors, this method can be defeated by a determined attacker if they have a sufficiently detailed copy of your fingerprint. Unfortunately, a copy of your fingerprint is not as difficult to come by as you might think. Just consider how many everyday items you touch casually, such as glass doors or windows, elevator buttons, cups or glasses, and any other non-porous surface.

▶

Face recognition – Front-facing cameras have been included on mobile phones and computers for many years, thereby making this technology appear to have the prerequisites for a mass-market deployment. In fact, this feature is already available on many phones, such as recent models running Google's Android operating system. Unfortunately, the current consumer versions of facial recognition technology still have a lot of room to improve. In its current forms, the facial recognition security locks depend on lighting conditions and facial expressions for their effectiveness and can be fooled by a simple photograph.

Possession Factors

Possession factors (i.e., what the user has) essentially rely on a key-and-lock system. The 'key' may take many forms, such as a keychain token, smart card or a small device designed to interface with the machine, such as a USB or audio port token. Possession factors are relatively uncommon on their own for computing security, although they are frequently used as part of a multi-factor or two-step system (something we'll touch on a bit later). The primary weakness of using a physical object as an authentication mechanism is that it may be stolen or damaged. Think of someone who has the keys to your home, for example; they would have unrestricted access to everything inside!

Knowledge Factors

Knowledge factors (i.e., what the user knows) are very commonly used, such as a secret PIN, pattern or password. The main common advantage to knowledge factors is that the 'secret code' may be changed with relative ease and frequency. For example, in most applications, changing your PIN or password only requires a couple of clicks. Among other things, knowledge factors can be vulnerable to what is known in the computer security world as "brute force attacks." Simply put, a computer program attempts to 'guess' a passcode by systematically trying a large number of various combinations in a short amount of time. Of course, the greater the number of combinations, the harder it is to crack a password in this way. This is why, despite the inconvenience to the user, longer passwords that use a combination of numbers, symbols and both upper and lower case letters are considered to be more secure. Unfortunately, the longer and more complex a password becomes, the harder it is to remember!

A four-digit PIN has 10,000 potential combinations; a six-digit PIN has one million.

PINs and patterns, commonly used by financial institutions and Google's Android operating system respectively, have the advantage of being easier to remember. Depending on the number of digits in a PIN or dots in a pattern, there may be fewer potential combinations. A standard four-digit PIN, for instance, has only 10,000 potential combinations. On the other hand, a six-digit PIN has one million. Patterns, as implemented in Android, however, have fewer possible combinations than PINs, mainly due to the number of dots, and the inability to "re-use" the same dot twice.

.....*continued on back page* ▶

PYC Briefs

Congratulations to **Susan DesLauriers, Executive Director, St. Matthew's Bracondale House.** Ms. DesLauriers won the draw for the Niagara Presents gift basket courtesy of Prentice Yates & Clark at the recent ONPHA Conference and Trade Show.

Best of Luck to Robert Wheater who has joined another accounting firm recently to further expand his experience. Congratulations also goes to Robert who has successfully completed the CICA Uniform Final Examination. Robert is now accumulating work experience toward his designation as a chartered professional accountant.

J. J. Pauze, Viola Bardhoshi and Dionne Reid will be attending the Co-op Staff Association of Central Ontario and Co-ordinators Association of Southwestern Ontario's 2014 Education Forum in February 2014 to be held at Ingersoll's historic Elm Hurst Inn. Viola Bardhoshi and Dionne Reid will be deliverying one workshop: **"Business Practices to Prevent Fraud".**

The Tools 2013 Conference for Non-Profits, Charities and Co-operatives was held November 20, 2013.

Dionne Reid, Viola Bardhoshi and Paul Jaroszko delivered two workshops: **"Demystifying the Audit"** and **"Internal Controls and Fraud"**.

David Robertson and Brian Iler presented a workshop on the topic of the implications and effects of the end of the operating agreements for the NHA Section 95 housing co-operatives. The discussion surrounded some practical accounting and financial consequences at the end of the agreements along with a good discussion about what the future held for these housing co-operatives and what their options were. Several possible scenarios were discussed with participants and there was general agreement to continue to examine the alternatives on a sector wide basis.

TAX NEWSFLASH

If you send CRA payments, you must also send a remittance advice.

Beyond the Password.....▶*continued from previous page*

Multiple Factors

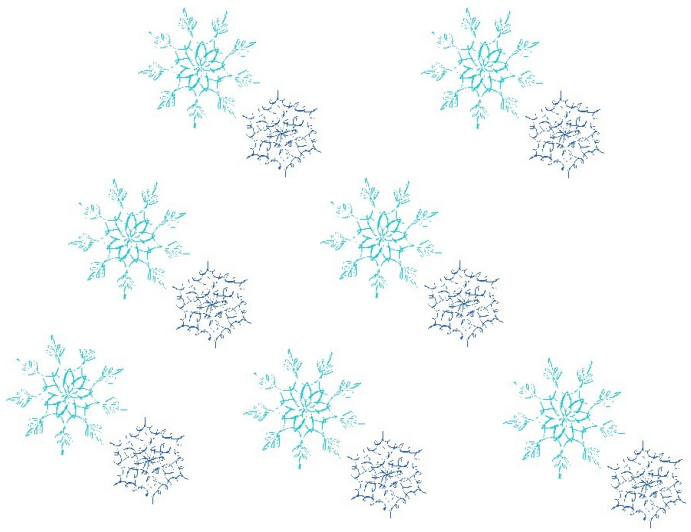
Since biometric-, possession- and knowledge-based factors all have weaknesses of some sort or another, data security teams have devised what is known as Multi-Factor Authentication to try to decrease the possibility that a data thief or "hacker" will be able to breach your security. Multi-factor (also called two-step or two-factor) authentication is intended to make it more difficult for an attacker to have all the required factors, thereby improving security. An ATM is a classic example of a security system that requires two-step authentication in order to complete any transactions. First, you require a debit card (the possession factor) and second, you must know the PIN (the knowledge factor). Multi-factor authentication is often a requirement for highly secured IT systems, although it is becoming more commonly available in consumer applications. Google, Facebook, Twitter and other major online sites are now optionally offering some form of two-step authentication as well.

While Multi-Factor Authentication is arguably far more secure, the limitation is that the system itself must be set up to use two-step authentication. Unfortunately, since most software programs don't have the option to add a second step for authentication, a password is the only option available.

Balance Security with Convenience

Security and usability tend to have a direct relationship: as data security increases, it often becomes more difficult to access the data. The trick is to find the right balance between an acceptable level of inconvenience and the desired level of protection for your data and privacy. Keep in mind what you're trying to protect and the potential consequences if someone gains unauthorised access, and use an authentication method that strikes the best balance. For example, your fingerprint may be secure and convenient enough to keep prying eyes from your personal email or Twitter feed, but you might consider using something more secure for your financial accounts or sensitive client data.

Regardless of the kinds of authentication you're using, a little common sense can go a long way. Use a password that's sufficiently secure, never share your PINs or passwords, and don't write them down! ♦



Winter 2013

Prentice Yates & Clark, Chartered Accountants

Phone: 416-366-9256 / Toll Free: 800-265-7818

Fax: 416-366-9171

Contact	Tel. Extension	e-mail Address
Partners		
Charlie A. Petralito	226	charlie.petralito@pyc.net
Lloyd K. Turner	235	lloyd.turner@pyc.net
Tom McGivney	233	tom.mcgivney@pyc.net
J.J. Pauze	230	jj.pauze@pyc.net
Retired Partner		
David L. Robertson	234	davidr@pyc.net
Accounting Staff		
Ahmad, Bakhtawar	238	bakhtawar.ahmad@pyc.net
Bardhoshi, Viola	239	viola.bardhoshi@pyc.net
Bell, Katya	236	katya.bell@pyc.net
Chohan, Preety	246	preety.chohan@pyc.net
Everett, Jessie	237	jessie.everett@pyc.net
Gatti, Garry	253	garry.gatti@pyc.net
Ho, Andrew	249	andrew.ho@pyc.net
Jaroszko, Paul	227	paul.jaroszko@pyc.net
Kiran, Sanjay	274	sanjay.kiran@pyc.net
Oza, Bhavin	251	bhavin.oza@pyc.net
Reid, Dionne	232	dionne.reid@pyc.net
Sharma, Rohan	231	rohan.sharma@pyc.net
Sundaralingam, Jesika	248	jesika.sundaralingam@pyc.net
Tozer, Colin	245	colin.tozer@pyc.net
Administrative Staff		
St. Louis, Carole	228	carole.stlouis@pyc.net
Palmer, Shannette	242	shannette.palmer@pyc.net
Colleen Pereira/Reception	221	reception@pyc.net

visit our web site

www.pyc.net

We hope that you find *info@pyc.net* a useful source of information. If you should ever have any specific questions or concerns regarding your own business or personal finances, please call us. We will gladly help in any way that we can. If you would like to contact us by e-mail, we can be reached at info@pyc.net. Some of the articles appearing in this issue of *info@pyc.net* were prepared by the Chartered Professional Accountants of Canada for the clients of its members.