K J HARRISON
INVESTORS

WEALTH, HEALTH & KIDS™

PROTECTING YOURSELF FROM CYBER CRIME

Crime is a lot like a beach-ball in a swimming pool. You can push it down to the bottom, but it will slip through your hands and resurface somewhere else.

Street crime is falling - thanks in part to the fact that fewer people carry cash. The bad news is, the criminals have moved online; a place from which they can tap into our most sensitive personal and financial information.

Recently, KJ Harrison worked with Canada's foremost financial services research provider, Strategic Insight (formerly Investor Economics), to publish a white paper on, ***The New Attitudes and Expectations Among High Net Worth Canadians***. A top response was cyber security – people felt their increasing reliance on computer networks made them vulnerable.

So, given that the first step in preventing cyberattacks is awareness, we spoke with several cybersecurity experts from the legal, technical and law-enforcement worlds to get their perspectives on ways our clients can minimize the risk of these emerging threats. On May 31, 2017, we hosted a panel on cybersecurity with **Imran Ahmad*, a Business Law Partner at Miller Thomson** who leads the cybersecurity, data protection and privacy law practice at his firm; **Larry Keating*, President and CEO of NPC**, which specializes in secure computing and **Kenrick Bagnall*, a Detective Constable and Cybercrime Investigator with the Toronto Police Force**. For a link to our panelist biographies please click here. The following paper is a summary of the panel discussion. The article takes you behind the headlines to give you a better understanding of what damage is being done online and what can be done to protect against such risks.

Cybercrime Defined*

While the typical image of a hacker is a teenager in a hoodie trying to break into networks to steal saleable information, the reality is starkly different. Most modern hacking operations are set up like businesses and go far beyond trying to grab credit details with an eye toward scoring a few purchases before the card company shuts them down. It could actually include clicking on a link and having your computer completely encrypted, or further still the wiring of funds to an account by accident because somebody was pretending to be someone else. This is an incredibly lucrative kind of criminal act. A recent FBI report values thefts from network breaches at $5 billion during 2016 alone. The Obama administration announced in 2010 that cybercrime had surpassed the illicit drug trade as the most lucrative crime in the world.

Cybercrime also has regional footprints. Criminal harassment tends to originate in Asia, low-dollar online fraudsters generally operate in West Africa, and high-dollar fraud and politically motivated hacking generally comes out of Eastern Europe.

*Please note by clicking the header links in blue you will be taken to this section of our KJH Managing Risk: Cyber Security and Technology Panel Webcast.

The majority of cybercriminals are looking for easy targets, note our experts, so a little prevention goes a long way to keep yourself safe. The panelists offer these nuts-and-bolts suggestions for avoiding hackers:

Inventory Your Technology and Online Behaviour*

A big barrier to maintaining cybersecurity is coping with the extent to which technology infiltrates our lives. As Ahmad notes, everyone now watches TV on phones and tablets and, "There's no way we're going to voluntarily go back 20 years to when people didn't have these mobile devices."

Technology underpins everything we do – education, entertainment, healthcare, work. So, the first line of defense is to carefully inventory all the devices you use each day.

"I've got this computer. I've got this smartphone. What am I doing online?" says Keating. "Start your own little list of what you do, and that will help you identify the things you should be doing in the future to help protect that process."

Get Serious About Passwords*

Never use the same password for more than one online service. That rule applies even if you have devised a 30-character password you're convinced no-one else can guess.

To remember your passwords, says Keating, "Build your own little hack where you use a standard phrase and then something that won't name the service but will remind you of that service; and then some numbers that make sense to you." That process creates a logic around the password to help you remember it, but preserves a level of randomness that will protect you if someone guesses your key phrase.

The reason you should not re-use passwords is that every web service has different internal security standards. That means you can have a hardened password, but if a hacker can phish it from one of those weaker services, you will no longer be protected on the more secure sites you use – including those where you make financial transactions.

Bagnall advises against default passwords like "123," which is apparently the most common in North America, and never using kids', grandkids' or pets' names. And, as for remembering the phrase, he says in all seriousness, "The best password manager is between your ears."

Hire the Right Experts*

Not everyone is technical. If you're not, get help.

Most people don't do their own lawyering or accounting. They should apply the same rule to devising cybersecurity systems. It doesn't make sense to do everything yourself when there are companies that make it their business to set people up with ultra-secure computers. And those same companies can perform high-end hardware upgrades – including biometric logins – that facilitate the use of ultra-complex passwords.

*Please note by clicking the header links in blue you will be taken to this section of our KJH Managing Risk: Cyber Security and Technology Panel Webcast.

"Does anybody look under the hood of a car anymore?" asks Keating. "I used to do that 30 years ago but I don't anymore because somebody else put that car together and made it work. Don't force yourself to become super technical."

Get Products that Secure You Properly*

Optical identification tools provide a solid workaround for people who are concerned their long pass-phrases will one day lock them out of their own computers.

Keating says biometric fingerprint readers, which now come standard with higher-end machines, can also be added as an aftermarket accessory. "Let's say you put in this crazy-long password about something funny your kid said at Disneyland, and then after that to get into your computer you're swiping your finger," he says. "We call it single sign in."

Don't worry, though. Just because your fingerprint is in your computer, that doesn't mean a hacker can then steal it. The better technology immediately converts the scan into a mathematical algorithm, which cannot be reversed into an image.

Encrypt Your Tech*

Security needs are largely dictated by what's kept on a computer. If you use it to run a business, store files containing deal data, or sit on a corporate board, the machine should be encrypted.

"If it's just the family pictures and you're not doing a lot financial stuff, you don't have to worry about encryption yet," says Keating. "Just get that long password and the fingerprint reader."

The upside of encryption – which mathematically scrambles data on your computer so that only a person holding the right certificate can unscramble it – is that it works. And, that's also its downside. If you encrypt, you need to ensure you have a failsafe to gain access to your password, and you also need to ensure the data are backed-up.

And, Keating adds, "If you have to compute mobilly, get embedded 4G wireless. It's secure."

Make Sure to Patch*

You've likely heard about the WannaCry virus – a piece of ransomware that, back in May, used an encryption code to lock up thousands of computers worldwide. The virus' creators demanded money in exchange for the certificate to release the infected computers. The virus wreaked-havoc, and even temporarily shut down a few hospitals while IT workers scrambled to sort out their systems. Ahmad notes these types of attacks, have "seen a tenfold increase over the past four years."

Funny thing, though, says Keating is that on March 14, Microsoft released a patch to protect computers running Windows systems from just that type of attack. "If everyone had patched their computers,

*Please note by clicking the header links in blue you will be taken to this section of our KJH Managing Risk: Cyber Security and Technology Panel Webcast.

nobody would have been hacked," he says, "but that's not how people think. This problem is in its very nascent stages."

Hackers are always looking for what he calls "zero-day opportunities" – a fault in a piece of common software that lets them into people's computers. "Vendors, when they find out about it, issue a patch that blocks them from accessing your computer that way," he says. "It's a race. So, if your computer hasn't been patched in six, eight, ten months or a year, you're going to have a problem."

The same goes for your phone. Bagnall notes all the major mobile operating systems frequently push out patches or system updates. They aren't just for functionality; a lot are for security. Take them.

Backup*

Which brings us to the next crucial piece of advice. The hackers who created WannaCry were by most accounts amateurs, and the certificates they sold to unlock people's computers didn't work consistently. Most victims who did recover only did so because they had their data backed up.

The lesson? One of the items on your technology inventory needs to read: Do I have a copy of everything I do on this computer somewhere else? If the answer is no, head to an electronics superstore and buy a three-or-four terabyte drive to place beside your computer. But, when you're done working, don't leave that backup device lying around. Store it somewhere secure.

"They have to be in different locations," says Keating. "God, forbid you have a fire, a flood or a break-in. They will steal the backup. They want both." Alternatively, consider a cloud service. This requires some homework, but there are good ones that will back your information up through the internet to secure facilities, and can meet your compliance requirements if you use the computer for business reasons.

Anti-Virus is a Must-Have*

Keating likens running a computer without anti-virus and anti-malware software to driving a car without a seat belt. "I actually heard a Microsoft executive talking almost 10 years ago, and he saw what was coming and he thought putting anti-virus software on your computer should be a civic responsibility," he says. "He felt there should be a law around it."

He adds it's critical to get a good product from a name provider like Norton, McAfee or Eset. Free software is a classic "you get what you pay for scenario," and that applies to everything from virus protection to word processing to file transfer.

What's more, anti-virus software needs to be installed on both work and home computers. "How many times do you come home from the office, and you didn't bring your laptop, so you do some work on the home computer?" he asks. "If there's a virus on there, you take it back to the office."

*Please note by clicking the header links in blue you will be taken to this section of our KJH Managing Risk: Cyber Security and Technology Panel Webcast.

Know Your Normal*

Here are some signs an email falls outside the definition of normal: It's from a bank you don't use and asks for account information or passwords; it's from a bank or financial services provider you do work with, but a click on the 'Privacy Statement' or 'Terms and Conditions' takes you to a different company's website; it's from someone you've never heard of offering to transfer a large sum of money into your bank account.

Bagnall stresses these types of emails aren't the kind you'd normally receive in day-to-day personal or work communications. They're from people who don't really know you; and by extension, are likely trying to scam you. Delete them, unopened.

"A lot of organizations don't understand what normal looks like in their network environments. Joe from IT is still there when it's 9 o'clock at night. He's not normally here," he says. "Understanding what normal looks like can make a huge difference. You stop and say, 'That doesn't look normal.' Because if it doesn't, it's not. It's an attack waiting to happen."

Keep Private Information Private*

Few people are truly aware of the size of their social media footprints.

Bagnall recounts a visit to a coffee shop near his office, during which he and his colleagues overheard a conversation between two women, one of whom (named Susan) had just qualified for the Boston Marathon. As an academic exercise, they decided to see what they could learn about Susan – knowing only her first name, what she looks like and that she'd qualified for the race.

It took 15 minutes for the team to learn much of Susan's life story, because she'd failed to privatize her social media. The officers knew where she lived, what kind of car she drove, her husband's name, how many children she had, how old they were, and where they attended school. "That took us 15 minutes," he stresses, "and we're the good guys."

Careful social media practices are doubly important for people with teenagers, who tend to photograph everything and put it online. To protect his family, Bagnall sets strict rules for his own two teenagers: No photographs of the outside or inside of their home – they make it too easy to lifestyle-profile the family; GPS trackers must be disabled; and his kids are told not to share their devices with friends – a common habit among millennials that makes them easy to hack.

Wash Your Web

A somewhat inconvenient, but effective, way to protect yourself from cybercrime is to create a paper trail – or in this case a data trail – that tracks your online activities. If you make online purchases, or sign up for streaming services or gaming, create separate accounts that you don't use for other purposes.

*Please note by clicking the header links in blue you will be taken to this section of our KJH Managing Risk: Cyber Security and Technology Panel Webcast.

"Get a separate credit card with a low credit limit. If it gets stolen, that number becomes a way to identify you," says Keating. "You have your credit cards for when you're out in the world, and a separate one for online. You're putting a firewall between your information."

You should also segment your email addresses and passwords for less-secure services, because many service providers use them as a unique identifier. "Every time you sign up for something they want your email address," says Bagnall, "and a lot of them use that as your account ID. So, I recommend a generic email address that you use for those services."

Be Smart About WiFi*

Public WiFi is a minefield, and hackers love to exploit the pock marks.

Ahmad tells of a recent visit to Toronto's Pearson Airport. All around him, people were catching up on emails or simply relaxing with a video while waiting for a flight; the majority using the airport WiFi – or so they assumed. He went to log in, clicked the access utility and found dozens of options for the airport. Some of those, he suspects, were a hacker's favourite information gathering tool: hotspots set up with mobile phones that masquerade as legitimate public WiFi.

"They created [a phony] WiFi access that had Pearson in there. It had the right three-digit code for the airport," he says. "And when you clicked on that you're connected [to the internet] but the individual can view specific pages, social media, other information. They can see the pages you're going through."

Certain clues give away spoof WiFi. Legitimate WiFi access automatically loads a 'Terms and Conditions' page, which you have to okay before you can get online. Click on a few links, because a lot of hackers are lazy and will use the 'Privacy Policy' and other legalese pages from a different company's site on the assumption that nobody checks. If those links don't go to the right places, don't log on.

In summary, cybersecurity clearly involves everyone in some manner. The consequences have a wide range of impact on governments, businesses and individuals. We, at KJ Harrison, accept that cyberattacks are increasing in frequency and magnitude. As an organization, we promote a strong KJ Harrison security culture and feel strongly about being prepared and having effective cyber-risk mitigation policies and procedures.

*Please note by clicking the header links in blue you will be taken to this section of our KJH Managing Risk: Cyber Security and Technology Panel Webcast.