

Working remotely has significant pros and cons

ACROSS THE CANADIAN automotive industry, working off-site has had distinct benefits and drawbacks that are guiding decision-making as to how permanent work-from-home measures will become.

ADVANTAGES

GREATER PRODUCTIVITY

Reduced commute times have allowed employees to be better rested, less stressed, and more productive. "I see a lot more throughput," said Maria Soklis, president of Cox Automotive Canada. "There are long commutes in Canada, in particular in Toronto and Montreal. [Now] there's a lot more time, greater flexibility, less stress around the workday."

GOOD FOR RECRUITING

John Trogakos, associate professor at the Rotman School of Management, said companies that are willing and able to adapt will see remote work on a part- or full-time basis as an advantage they can use to attract top talent. "I think it's a mistake for companies to write off a hybrid system, at least, because companies are going to start offering that as a perk," he said.

LARGER TALENT POOL

For certain positions requiring significant levels of skill or education such as R&D or engineering, being open to remote work can provide access to a broader talent pool. "That would be a huge benefit if you did have R&D and you had designers all over the world that could provide different creative ideas," said Hyundai Canada CEO Don Romano.

REDUCED OPERATING COSTS

If part-time remote work becomes permanent, "[Companies might] have the option of reducing physical space and saving costs there, and reducing the costs of things, like supplies [and] energy costs," Trogakos said.

DISADVANTAGES

DIFFICULTY BUILDING TRUST

Romano said his primary motivation for returning employees to centralized work is that teams have difficulty building trust when they're not working together.

"Once you get that trust factor going within a team organization ... it's hard to maintain that through Zoom [meetings]

and through these electronic systems," he said.

This assertion has a basis in science, according to Mahdi Roghanizad, an organizational behaviour specialist from Ryerson University's Ted Rogers School of Business. He told *CBC News* in a June 29 report that, "Eye contact is required to activate [trust among teams], and when the eye contact is not there, the whole other signal information is not processed by our brain."



Mahdi Roghanizad, organizational behaviour expert, says eye contact is key to establishing trust, which is something that a Zoom video meeting can't achieve.

PHOTO: RYERSON UNIVERSITY WEBSITE

LESS ACCESS

Another challenge is contact with co-workers.

"At work, you can just get up off your chair and walk to the person next to you and ask a question," said Todd Sheppelman, CEO of Toronto-based automotive plastics supplier ABC Technologies. "[During remote work], you had to call them up or schedule a conference call. And because everybody was doing that, people were much busier with meetings than they typically were."

REDUCED WORK-LIFE BALANCE

It can be harder to separate work and family life when an employee's office is at home. Cox Automotive Canada's approach is to offer financial assistance with setting up dedicated home office spaces where required.

Having a separate work space provides clearer separation — a literal wall — and reduces the feeling of always being at work, Soklis said.

Sheppelman said that early in the isolation period, employees were regularly holding conference calls in the evenings and logging into the company's secured network late at night.

"We tried to have it set up that there were normal work hours," he said. "Let's figure out how not to have conference calls from 7 at night. People do have a life that they're trying to live."

LACK OF HUMAN CONTACT

The one challenge that might truly be insurmountable is that some people no longer feel like part of a something bigger.

"I'm hearing from some of our people about how it's lonely, how they miss their colleagues," Soklis said.

"We've tried to hold training sessions, little social events, but it's not the same. There's a certain camaraderie and team spirit that you can't feel through a computer." — **ANC**



In home switch, companies risk exposing private data

Using personal devices or unsecured networks, or improperly discarding printed documents, can jeopardize businesses

By **STEPHANIE WALLCRAFT**
TORONTO CORRESPONDENT

REMOTE WORKERS COULD BE exposing their employers to contractual violations and legal disputes if they are not correctly handling sensitive information.

For the automotive industry, particularly within the automaker-supplier relationship, trade secrets often comprise the highest-risk information.

Trade secrets are defined by the Canadian Intellectual Property Office as "any valuable business information that derives its value from the secrecy." This can include a formula, process, technology, design or other asset that is not or cannot be legally protected through other methods such as acquiring patents.

When a company-owned trade secret is exposed, the lost value is unrecoverable. This becomes especially complex when one company's employee exposes a trade secret belonging to a third party — for example, an employee of a Tier 1 supplier inadvertently makes an automaker's trade secret public knowledge — which can put that employer at risk of a legal battle over breach of contract.

"There can be legal obligations pursuant to those contracts ... if appropriate steps aren't taken to ensure that those [trade secrets] are properly protected," said Lyndsay Wasser, co-chair of the privacy and data protection group and the cybersecurity group based in the Toronto office of multiservice law firm McMillan LLP.

Employees must be trained on how to verify that data is encrypted whenever being transmitted or stored, and must also understand that sensitive data should never be downloaded to personal devices such as smartphones or personal computers, said Wasser.

"Typically, we would want that information to be maintained within the

company's networking systems," he said. "That can be difficult if employees are using personal devices to work from home where the company wasn't able to provide company-issued laptops and other technology."

SECURE NETWORKS

Ensuring that employees understand the distinction between secured networks and unsecured personal email accounts or other cloud-based apps, particularly those not approved by their employer, is critical.

"We're starting to see [automakers] getting very prescriptive on where you can place documents," John Heaton, a Toronto-based partner in the cybersecurity advisory services practice of accounting firm KPMG, said in a webinar on cybersecurity hosted by the Automotive Parts Manufacturers' Association on May 7.

"The German [automakers] in particular have a very specific set of rules you have to follow and encryption that's required. ... If you're using a [cloud-based] solution, there may not be any encryption of that data."

Companies should also ensure that their secure networks require login using multi-factor authentication, such as a password in combination with a code sent to a smartphone, to validate employee identity.

"Multi-factor authentication provides that extra level of security in case the password itself is not strong or has been previously compromised," Wasser said.

While the current working environment places an emphasis on technology, Wasser said companies should not overlook the low-tech risks of working outside of a centralized office such as leaving printouts exposed on home workstations or in municipal recycling bins.

"It is advisable to limit hard copies as much as possible because many individuals don't have the appropriate facilities to ensure that information is properly protected in a home environment in terms of locked cabinets or shredding facilities," Wasser said. "Organizations ... should have procedures and rules in place for employees handling information in that form." — **ANC**



Wasser: Companies have to guard against low-tech risks such as leaving printouts on display at home offices.

FILE PHOTO



Heaton: Automakers are making rules for their employees on how to store documents securely.

FILE PHOTO