DIGITAL JOURNAL

CIO ASSOCIATION OF CANADA

A NATIONAL CELEBRATION HONOURING CANADA'S MOST EXCEPTIONAL TECHNOLOGY LEADERS









The innovators shaping Canada's digital future

Presenting the Winners of the 2026 CanadianCIO of the Year Awards









Recognizing the leaders bringing people through change



Derek Cullen, CIO.D, president & chair, CIO Association of Canada

Every generation of technology leaders has had to bring people through change. This one is doing it at a speed none of its predecessors faced, with new tools arriving faster than most organizations can absorb them, and with the accountability resting on the technology leader long before the rest of the business has caught up.

This year's award recipients run technology for an aerospace manufacturer, a pension investor, a physician regulator, a power utility, and an auto group, and each of them treated bringing people along as the central part of the job. They walked the plant floor to see how work gets done, gave colleagues outside IT the tools and the confidence to build, brought operations and business leaders into decisions from the start, and made sure their own teams were taking the time off they needed.

The stories that follow show what that leadership looks like inside very different organizations, and why the change that lasts in each of them began with people.

Shaun Guthrie, our past president and chair, made that case to this community for years. He often said technology was never the hard part, and that the real work was understanding the business it serves. We lost Shaun in June, but his legacy lives on through leaders who share that conviction. This year's recipients are a testament to that legacy.

On behalf of the CIO Association of Canada, we thank our sponsors Red X Carbon, Zoho, Armadin, QRX Technology Group, and Lenovo, whose support makes this recognition possible.

Congratulations to this year's recipients. Your decisions have a lasting impact on your organizations and the people who depend on them, and we're proud to recognize the leadership behind them.

Derek Cullen
President & chair
CIO ASSOCIATION OF CANADA

Lorraine Bauer
Executive director
CIO ASSOCIATION OF CANADA

Photography by Jennifer Friesen, Digital Journal

One purpose.
One Lenovo.

Smarter technology for all

Lenovo



Turn your AI vision into reality with a trusted enterprise partner.

lenovo.com

Years of data cleanup bought this regulator an AI head start

Eben Engelbrecht, CIO.D

Director of information technology and facilities

COLLEGE OF PHYSICIANS AND SURGEONS OF ONTARIO

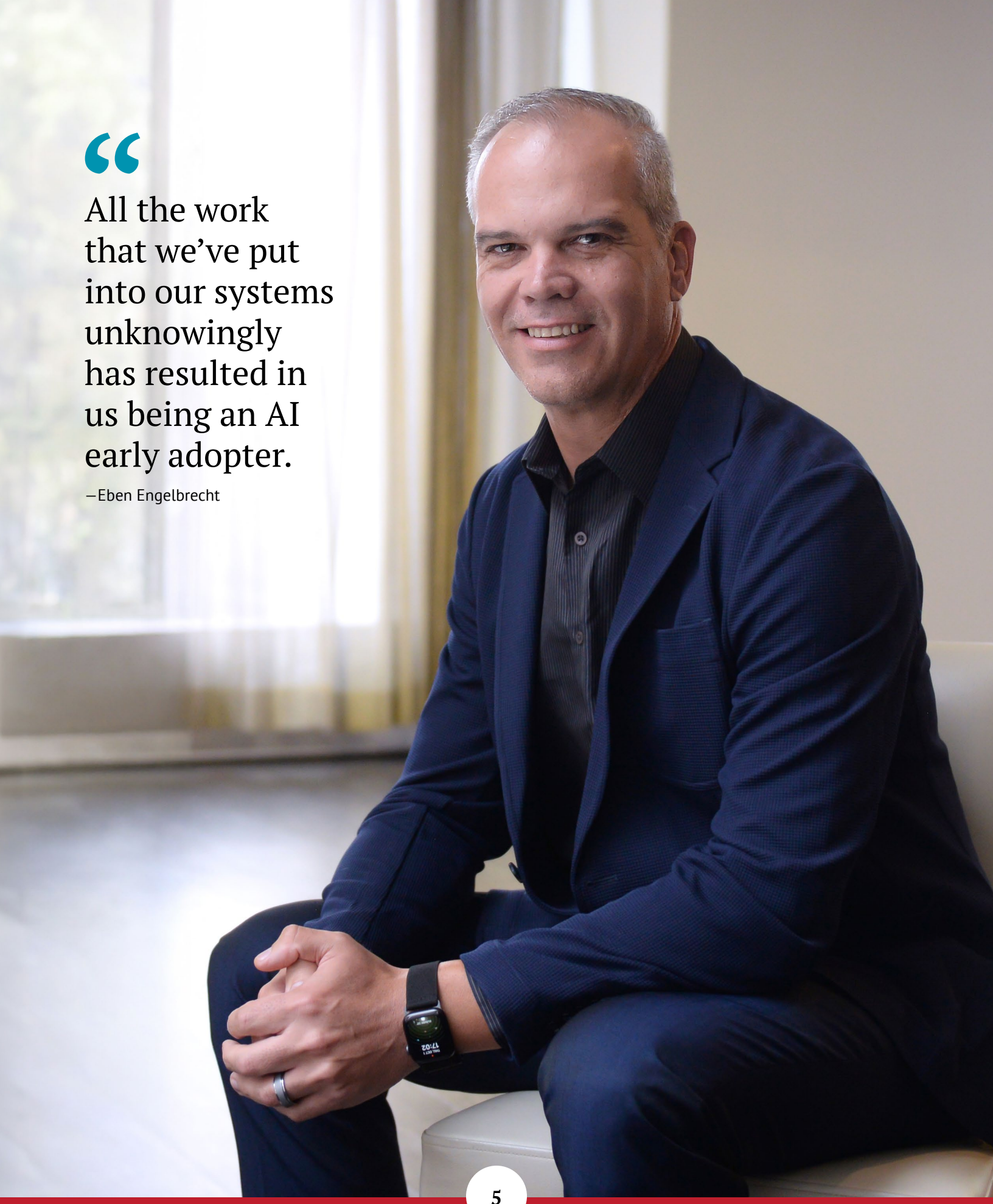
A decision letter from Ontario's medical regulator can affect a physician's ability to practise. For years, the people who wrote those letters built each one by hand, some starting from scratch, some from a template, copying material in and out of the file.

Eben Engelbrecht's team now has AI produce the draft. A decision writer reads it, fixes it, and submits it.

Engelbrecht is director of information technology and facilities at the College of Physicians and Surgeons of Ontario (CPSO), and the winner of CIO of the Year in the not-for-profit category at this year's CanadianCIO of the Year Awards, hosted by the CIO Association of Canada.

"They're ultimately responsible still as the drafter to then submit it," Engelbrecht says. "The AI is not making the decision for them. The AI is purely just giving them the information that already exists. No decision-making is happening."

Getting there took almost six months of training the model, he says, working through the business until it held up. Accuracy sits in the high 90s, and odd cases still need a person to pull in material the model missed.



> All the work that we've put into our systems unknowingly has resulted in us being an AI early adopter.
>
> —Eben Engelbrecht

Despite having staff out on vacation and parental leave this summer, decision writers stayed on pace with their targets anyway, which Engelbrecht credits to spending less time copying, pasting, and assembling documents by hand.

Reporting drove the data cleanup

When Engelbrecht joined CPSO, the college was running 32-bit Windows machines and WordPerfect, with roughly 700 servers running on Nutanix hardware in an on-site equipment room and no cloud presence.

Moving to a Microsoft cloud environment and a member portal took years, and much of that time went into cleaning up the data.

Every database correction went to one person, who typed it in by hand.

"We had the Yoda sitting at the back end fixing data manually," Engelbrecht says.

A Yoda is a useful thing to have right up until you need two of them. The record stayed only as consistent as one person could keep it, and it held what Engelbrecht estimates was close to a century of physician registrations.

CPSO needed that data structured to report complaint timelines, physician locations, and regulatory outcomes to government and the profession, long before AI had anything to do with the project.

Data cleanup consumed almost half the project time.



Eben Engelbrecht is the director of information technology and facilities at the College of Physicians and Surgeons of Ontario

When Microsoft ran an AI readiness assessment on CPSO's systems, the college hit the mark on the strength of work finished years earlier. That result helped make CPSO one of Microsoft's frontier firms.

"I knew that was going to be the case," Engelbrecht says. "All the work that we've put into our systems unknowingly has resulted in us being an AI early adopter."

The controls came before the AI

Engelbrecht traces the college's approach to security back to a cyber incident early in his tenure, while CPSO was still running on-site servers. The systems it hit had already fallen out of active use.

The incident, he says, made the case to his board for investing in cybersecurity.

The first question it asks a prospective vendor is where its data resides. Multi-factor authentication, the second code you enter after your password, rolled out to the physician portal in phases so members could adjust before it became mandatory.

Engelbrecht's team wrote the governance and policies first. Staff were already experimenting with ChatGPT by the time that work started, and the risk he wanted closed was private physician information going into a public model CPSO didn't control.

Copilot started as a pilot with staff representing every department. Once that group was comfortable with it, CPSO rolled it out to everyone else.

"We don't have to rush into AI," he says.

He credits the lunch and learns for the uptake, saying he could watch adoption move in the data right after each session. Across just under 400 staff, it reached 94% to 95%.

> "We were really lucky and we were ready when that legislation passed.
>
> —Eben Engelbrecht

A deadline with no room to miss

In 2025, the Ontario government handed CPSO a legislated deadline to start regulating physician assistants, a new group of roughly 1,000 members alongside the college's 50,000 physicians.

Engelbrecht's team adapted the registration system, member portal, and public register already built for physicians, work that predated the legislation by years. The new group was a fraction the size, but Engelbrecht says standing up the same core functions still meant roughly the same amount of work.

"We were really lucky and we were ready when that legislation passed," he says.

He uses that word a lot.

The cyber incident hit systems it had stopped using, lucky the cloud move was underway, lucky the registration work was built before the legislation arrived. Most of that luck took years to build.

DIGITAL JOURNAL

Scan QR code or click to watch **Eben Engelbrecht** and fellow not-for-profit finalists in a Digital Journal roundtable.

What comes first when cybersecurity never ends?

Rob Antonishen

Director of cybersecurity and compliance

B.C. HYDRO

Ask Rob Antonishen what a normal week at B.C. Hydro looks like, and he gives the same answer as nearly every other office worker.

"Meetings and emails," says Antonishen, director of cybersecurity and compliance at B.C. Hydro. "I think that's the modern reality for most people in this day and age."

Many of those meetings are about deciding which cyber risks the utility can live with.

Some of B.C. Hydro's systems are more than 30 years old, and Antonishen can't apply every security best practice to every one of them.

Antonishen won CISO of the Year at the 2026 CanadianCIO Awards.

Compliance is part of his title because B.C. Hydro must meet mandatory cybersecurity requirements for the North American power system.

"Compliance is not the same as security," he says.

Days before speaking with Digital Journal, Antonishen was in a large session with one of B.C. Hydro's operational technology groups. His message was that meeting those requirements is only the beginning of the job.

"These regulatory requirements are the low bar," he says. "They are not the ceiling when it comes to cybersecurity controls. They are the bare minimum."

Antonishen joined B.C. Hydro in 2021, leading a cybersecurity team in a role that hadn't existed yet.



> These regulatory requirements are the low bar. They are not the ceiling when it comes to cybersecurity controls. They are the bare minimum.
>
> —Rob Antonishen

> We have to design our systems to deal with somebody with malicious intent, somebody coming in to try and break the system.
>
> —Rob Antonishen

"They didn't have a single person who was accountable for cybersecurity for the organization," he says. "It was sort of an on-the-side-of-the-desk function for infrastructure."

How he decides what gets protected first

Before Antonishen can decide what comes first, he has to accept that not everything can.

"We have systems, some of them dating back 30-plus years from a technology platform perspective, and it's impossible to boil the ocean," says Antonishen. "We can't bring everything up to the modern levels of ideal cybersecurity protections and controls."

The most critical and exposed systems go to the front of the line. Where other controls already provide a buffer, Antonishen can accept more risk and focus his team somewhere else.

He makes those calls with the operations people, instead of trying to work around them, because a cyber risk sits next to an outage risk and has to be weighed against it.

Antonishen came up through operations, starting in protection and control at Ontario Hydro, so he and the people running the system already speak the same language.

"We are victims of our own love of technology in cyber and in utilities as well," says Antonishen. "We have our own language. We have our own terms. We love our three-letter acronyms and our four-letter acronyms."

A board has little use for a change in the patching rate or the number of blocked emails.

"You really need to focus on narrative, on storytelling, on allegories," says Antonishen.

So a phishing takedown stops being a phishing takedown. His team recently found a set of fake B.C. Hydro billing sites and worked with a takedown service and government agencies to shut them down.

"When I take that to the board, though, I say, look, we are maintaining our customer trust by doing that," says Antonishen.

Operational technology design has to account for malicious intent

Antonishen is a professional engineer licensed with Engineers and Geoscientists B.C. He is trying to bring cybersecurity into operational technology (OT) design from the start, alongside the reliability and safety work engineers already do.

"Historically the focus has been on reliability from a technical perspective, from an operations perspective," says Antonishen.

Engineers already design for equipment failures and storms. Antonishen wants it to account for someone deliberately trying to break the system too.

"We have to design our systems to deal with somebody with malicious intent, somebody com-

ing in to try and break the system," says Antonishen. "That's just something that is often not taught in this field."



Rob Antonishen is the director of cybersecurity and compliance at B.C. Hydro

What used to be the emergency is now normal

"For quite a number of years we had been holding ourselves as sort of an elevated threat level when it comes to cyber specifically, just because of what was going on in the world," says Antonishen.

Antonishen and his staff eventually stopped expecting the threat level to fall, so the precautions they put in place became part of the regular job.

"All of these things that we've been building and putting in place are now our new baseline. I think this is where we've seen the biggest change," says Antonishen.

And AI enters the conversation again as Antonishen says attackers use it to find vulnerabilities and run attacks that adapt to security controls.

"They can react to what your security controls are doing. They can pivot. They can shift," says Antonishen. "You're now battling against a more human attacker, and they can do it at scale."

B.C. Hydro uses AI in its security tools to sort through the noise and flag the threats his team needs to look at.

"There's so many things coming at us from all these different directions. It becomes almost overwhelming at times," says Antonishen, running through technology, geopolitics, vendor relationships, and supply chain risk.

The workload keeps growing, and Antonishen says the people drawn to cybersecurity are often reluctant to leave a job unfinished.

"They want to see a job done," he says. "They want to see things through."

He and his direct reports talk directly with staff about emotional health, mental health, and work-life balance. They ask people whether they've taken time off and whether they need more.

Antonishen knows what overwork can do.

"I personally went through a pretty nasty bout where I did burn out, and it was largely due to overwork," says Antonishen. "It's very close to me to make sure that doesn't happen to the people who look up to me and work for me. I can't afford for them to wear themselves out."

The rulebook covers the systems, but there isn't a section for the person still reading alerts at 2 a.m.

DIGITAL JOURNAL

Scan QR code or click to watch **Rob Antonishen** and a fellow CISO of the Year finalist in a Digital Journal roundtable.

Why this CIO won't let an AI agent take the blame

Brigitte Larivière

Vice-president and chief information officer

BOMBARDIER

Not long after Brigitte Larivière became Bombardier's CIO in 2022, she walked the manufacturing floor and asked aircraft workers what IT support was like for them.

They told her they had no phone near the aircraft. When something went wrong, they had to find one, call the help desk, and track down an asset number. If the help desk called back while they were working on the plane and missed them three times, the ticket closed.

"I don't want you to go for a phone. I don't want you to have any discussion with IT," Larivière told her team. "You have a problem, you raise your hand, or you go to the tech bar."

She put technicians on site so workers could get help where they worked. Her instruction to them was just as direct: "Your job is on the aircraft."

Larivière, Bombardier's vice-president and chief information officer, is the winner of the 2026 CanadianCIO of the Year Award in the private sector category.

The model was popular enough that head office staff asked for one too. Now they queue for service, and Larivière is working on an Apple-style booking system to manage the demand.

Look at what's happening before deciding what to fix. That instinct runs through much of what Larivière has done at Bombardier.

She spent her first decade at the company on the manufacturing floor, working the cockpit and electrical lines up to a supervisor role, before an SAP implementation pulled her into IT. She



> An agent is technology. It's a machine. At the end of each of those processes, we have to have a human that's accountable for all the agents under that.
>
> —Brigitte Larivière

thought she'd work on a few major projects and then return to manufacturing.

Her CIO at the time had other plans.

Larivière knew the product, the processes, and the people. More importantly, her CIO told her she could explain technology in a way the business understood.

The automation that doesn't need AI

Robotic process automation (RPA) uses rules to handle repetitive digital tasks. Seven years ago, she told her team she wanted roughly 40 automated processes a year.

"You're crazy," they told her.

RPA is still running across HR, finance, and manufacturing, with governance built around it and savings that continue every year, Larivière says.

"It was like, oh my God. We got $7 million to $12 million a year, and they're still running," she says of the reaction when she eventually showed the finance team the numbers.

Bombardier's next automation push is centred on AI agents.

Every agent needs a name attached

Some of Bombardier's infrastructure work is outsourced, including the help desk, server management, and patching. With those contracts set to end in about two years, Larivière is looking at what should happen to that work next.

She has challenged her team to automate about 80% of that outsourced work by the end of 2027. More than 1,000 agents could be deployed in 2027, she says.

Her own team initially balked at the target. Now, she says, the technology is moving fast enough that a large portion of the work could be automated by the first quarter of that year.



Brigitte Larivière is vice-president and chief information officer at Bombardier

"I don't want to insource the task," Larivière says. "I want to automate the task."

In other words, she isn't looking to bring the same work back inside Bombardier for employees to do. She wants agents to take on the work that can be automated, while Bombardier brings the management of those agents in-house.

"If something fails, I don't want to hear it's an agent," she says. "An agent is technology. It's a machine. At the end of each of those processes, we have to have a human that's accountable for all the agents under that."

Before an agent goes into production, she wants a named person responsible for the outcome, how

it will be measured, and whether it continues to work as intended.

She expects that to create a new kind of job well beyond Bombardier.

Individual contributors could become managers of agents, deciding whether their AI workers are performing, which ones need replacing, and which ones should be retired.

Give people somewhere to build

Tell people they can't use something and some of them will find another way to do it anyway.

That's the logic behind Larivière's approach to citizen development, where employees outside IT build dashboards, applications, agents, and other tools for their own work.

She's even told her team to retire a familiar term for it.

"I want my team to stop calling it shadow IT," she says. "It has a negative connotation."

Instead, Bombardier gives employees access to a set of approved tools along with training and a community of practice.

The company can then measure what's being built, see whether those tools are being used, and step in when people are operating outside the guardrails.

"You cannot stop people from being creative and innovative," Larivière says. "If you try to stop them, they'll find another way to make it happen."

The risk she worries about most

Cybersecurity is the area Larivière worries about most as experimentation and automation accelerate.

She points to research she says found 60% of cyberattacks involve a human somewhere in the chain.

> "You cannot stop people from being creative and innovative. If you try to stop them, they'll find another way to make it happen.
>
> —Brigitte Larivière

"I have a team of experts, and they're so good and so engaged," she says. "What I cannot manage is people not giving me the truth or hiding information. Everything needs to be said, put on the table."

The company now sells luxury aircraft to wealthy customers and is growing its defence business, which Larivière believes makes it more attractive to different kinds of attackers.

Quantum computing ranks lower on her list for now. Bombardier has begun internal discussions about encryption, where quantum could affect its systems, and what options it may eventually need, says Larivière.

Cybersecurity is the more immediate concern.

"How do you keep up with the pace?" asks Larivière. "How do you protect your company? How do you make people knowledgeable about the risk they're creating?"

DIGITAL JOURNAL

Scan QR code or click to watch **Brigitte Larivière** and fellow private sector finalists in a Digital Journal roundtable.

What happens when the business buys in

Tony Payne

Senior vice-president of technology and innovation and chief technology officer

BRITISH COLUMBIA INVESTMENT MANAGEMENT CORPORATION

Tony Payne and I are only a few minutes into our conversation when he starts laughing. He's more than two decades into a career he's reinvented more than once.

"When I grow up, I'll know what I want to be," he says. "I'm not there yet."

So far, that has taken him through software development, cybersecurity, IT and financial auditing, general management, and technology leadership at organizations on two continents.

Payne is senior vice-president of technology and innovation and chief technology officer at British Columbia Investment Management Corporation (BCI), and the winner of the 2026 CanadianCIO of the Year Award in the public sector category, presented by the CIO Association of Canada.

At BCI, the technology team doesn't have to go looking for problems to solve.

Their private equity department wanted to know which companies in BCI's portfolio might be able to sell to one another. Payne's team built a portal that mapped what the companies sold and showed where the matches might be.

"If I look at my career, technology typically tries to find a problem to solve," says Payne. "What I find here is, it's great to be in a position where the appetite and the pull is coming from the business that they can't get enough of technology."


“
When I grow up, I’ll know what I want to be. I’m not there yet.
—Tony Payne

> I've always been thinking, how do you do something different? If there's a process, there must be a way that you can do it differently.
>
> —Tony Payne

The business brings the use cases

BCI, an institutional investor, managed $313.7 billion in gross assets as of March 31, 2026.

Its investment decisions affect more than 818,000 pension plan beneficiaries.

Payne prioritizes the people behind those numbers.

"That is why we exist," says Payne. "That's why we always say the money we manage isn't ours. It's our clients' money."

He describes the work as a partnership between the people who know the business problem and the people who know how to build the tool.

Learn the business before you push the boundary

Payne joined BCI in February 2020 after taking the scenic route through technology leadership.

He started his career in software development and cybersecurity before joining a South African hospitality and casino company, where he led IT audit and later oversaw an IT division.

At one of those casinos, Payne spent three hours in a locked cash-counting room as one of three people in suits watching staff follow every procedure exactly.

With the auditors sitting there, why wouldn't they? He proposed reviewing randomly selected surveillance tapes instead.

"I've always been thinking, how do you do something different?" says Payne. "If there's a process, there must be a way that you can do it differently."

When Payne arrived at BCI, he started by building relationships across departments. He also created an innovation committee with a lead from each department, which he chairs. The group looks at process and product innovation as well as the culture around it.

"Innovation, in a way, is broader than technology innovation," says Payne.

One lesson he's taken from his career is to "stop being a techie," he says. Talk to the business side in its own language, build credibility by doing what you said you would do, and then push the boundary.

He expects the same of his own team.

"If you're not paddling, you're going to flow downstream," says Payne. "You have to paddle, and you have to have a team around you that can paddle together faster, so you actually go upstream."

From a leadership perspective, there's a balance between making progress and having guardrails that gives the team the "freedom to experiment and accelerate."

The demand shows up in how BCI staff use what Payne's team builds. His group supports AI work across the corporation through a three-tier model. They will do the work for you, do it with you, or train you to do it yourself.

Payne says about 95% of BCI staff use AI every week. On top of that, close to 30% of the com-

pany does some form of code development, and most of those people aren't developers.

At a recent internal hackathon, more than 20 teams competed and three-quarters came from outside the technology group. Payne's group was outnumbered three to one at its own event.

There are worse problems for a CTO than too many non-techies building things.

What the business asked for

The projects and the model behind them have already earned BCI two industry awards.

BCI's I2Pay system uses AI to scan invoices, pull the data, check it against accounting records, and route it through approval. The system cut processing time and duplicate entry, and reduced the number of DocuSign licences BCI needed.

I2Pay was recognized at CIO Awards Canada last year, and BCI's broader approach to innovation earned it an Innovator of the Year 2025 award from Info-Tech Research Group.

That's a respectable trophy haul for an invoice workflow.

Another project automates risk analysis for companies in BCI's portfolio.

The system ingests financial and competitive information for every company in the portfolio, extracts data from analyst memos, models the risk, and returns a rating.

Payne says work that once took two weeks now takes a day.

The team is also looking further ahead with quantum computing.

The security problem starts before quantum computers are ready. Attackers can steal encrypted data now, hold onto it, and decrypt it later once the computing power catches up. The industry calls it "harvest now, decrypt later," which is about as reassuring as it sounds.

Google has set 2029 as its timeline for migrating to post-quantum cryptography. Payne wants his team ready before the clock runs down.

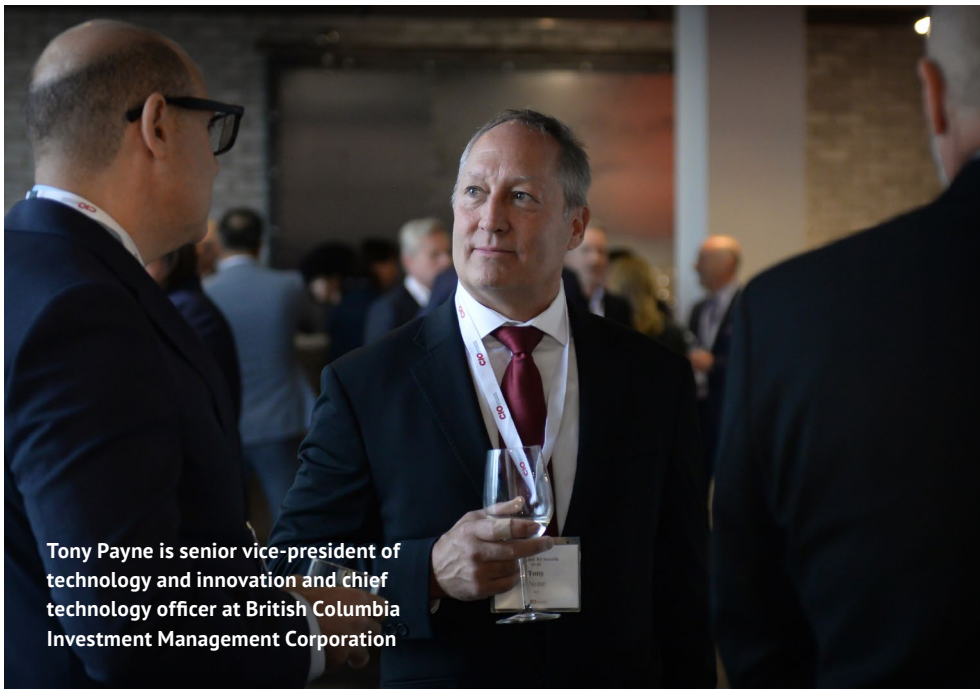
"I'm not passionate about the technology itself," he says. "While I've been in technology my whole life, what I'm passionate about is the innovation."

Payne says he used to "get bored" quickly and would often change roles every two to three years. But six years in at BCI, he hopes to stay another 10.

Evidently, not knowing what he wants to be when he grows up is working out.

DIGITAL JOURNAL

Scan QR code or click to watch **Tony Payne** and fellow public sector finalists in a Digital Journal roundtable.



Tony Payne is senior vice-president of technology and innovation and chief technology officer at British Columbia Investment Management Corporation

When the IT job becomes the risk job

Jennifer Hutton, CIO.D

Vice-president of information technology and risk and chief privacy officer

STEELE AUTO GROUP

"I'm the sort of person if I get 24 out of 25 on a test, I will challenge it because that's just not acceptable," says Jennifer Hutton, vice-president of information technology and risk and chief privacy officer at Steele Auto Group.

Hutton is the winner of the 2026 CanadianCIO Fawn Annan Memorial Award, given each year to a woman in IT leadership by the CIO Association of Canada.

She never planned a career that would put her up for it.

That refusal to leave the last mark on the table is how a job about technology and cybersecurity became one about everything that could go wrong at the company.

Hutton was hired to run IT and look after cybersecurity. Now, she also runs insurance, privacy, health and safety, and she's responsible for managing risk across the whole business.

She joined Steele in late 2022, her first job in the car business. The auto group is based in Dartmouth, Nova Scotia, and runs about 60 dealerships across the four Atlantic provinces and in Texas, with an IT team of nine.

Selling cars means selling to the public, and that changed what she had to protect.

A dealership holds the kind of personal and financial information a bank does, and the industry was slow to treat it that way.

"I called another dealership on P.E.I. and I said,



“I’m probably one of the few CIOs that will tell you I don’t block shadow AI.

—Jennifer Hutton

'Hey, we're getting some spam from your domain and do you have an IT department or somebody who looks after IT that I can speak to,'" says Hutton. "And the receptionist said, 'I don't know, I think our owner's nephew helps us on weekends, but I don't think he's available during the week.'"

Because that was normal, the software companies dealerships buy from were used to easygoing customers. When Hutton pushed them for stronger security, the managers and directors she first dealt with told her to back off.

"I was met with things like, 'That's not the way we do it. You came from outside the auto world, that's not how we do it here. Relax. It'll be fine. Go away,'" says Hutton.

Steele also grows by buying other dealerships, and Hutton won't let a newly acquired store run on its old systems for even a day.

"If the deal's closing on Sunday morning, the store closes 5:00 Saturday night. By 5:00 Sunday morning, they have all of our infrastructure, all of our systems, everything switched over," says Hutton.

Preparing for the outage before it happens

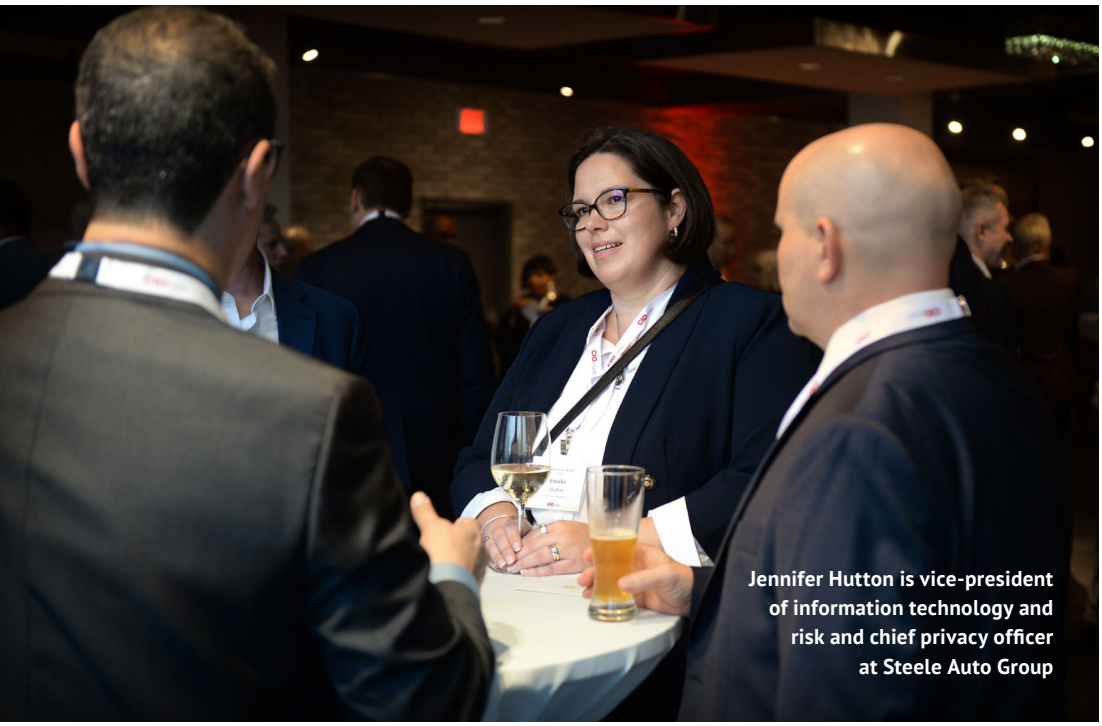
In 2024, a company called CDK Global was hit by ransomware.

Steele was ready when it happened. Hutton and her team were at The Keg the night the attack hit, prepping a tabletop exercise.

The scenario she'd planned was the dealer management system going down.

"We actually got to deal with the real scenario and the made-up scenario all in the same week," says Hutton.

The attack affected nine Steele dealerships for about two and a half weeks. They managed to keep taking payments the whole time, using backup systems the team had set up before anyone needed them.



Jennifer Hutton is vice-president of information technology and risk and chief privacy officer at Steele Auto Group

"The insurance company kept asking me, are you sure you're not making a claim for business loss," says Hutton.

She told them no.

Paying for that kind of preparation means keeping the technical detail out of the conversation with the board.

"Don't walk into a boardroom and ask them if you can buy a new firewall, because number one, they don't know what a firewall is," says Hutton. "Number

two, we don't want them to touch our firewalls."

What moves a board is the effect on the business. She turns every request into a plain question. How would the company run payroll if the systems went down? What would a shutdown of the dealer management system cost the group?

> Don't walk into a boardroom and ask them if you can buy a new firewall, because number one, they don't know what a firewall is. Number two, we don't want them to touch our firewalls.
>
> —Jennifer Hutton

Why she won't block shadow AI

Hutton treats AI as part of the company's overall risk.

"An AI strategy is not something that's owned by your IT department," says Hutton. "This is enterprise risk."

In her CIO association chapter, she says the common line is to block shadow AI until the rules and safeguards are ready.

Hutton allows it.

"I'm probably one of the few CIOs that will tell you I don't block shadow AI," she says.

Her reasoning is that people will use these tools no matter what, on a phone or a personal device if they have to, so she is focused on teaching them to use them safely.

The career she didn't plan

Hutton spent most of her career as the only woman in the room, or one of two. She's led technical teams made up of men for more than 20 years. Steele is the first place she's had women on her own IT staff.

She says she thinks the field stays lopsided because women don't apply, and they don't apply because nobody showed them it was an option.

"I remember the first time I saw a female airline pilot, and I went, huh, well, I would have done that if I had known girls could do that," says Hutton.

The Fawn Annan award makes her that example for someone else. It caught her off guard.

"When I really look back on the work that I've done, and my impact on people, I think is still what surprises me the most," says Hutton.

Hutton has built a career being described as someone who manages through crisis and change. Systems that fail, industries that lag, a board that needs convincing. She has a method for all of it.

Then the last year handed her something no method covers. She lost her mother and her husband within months of each other.

"This is one of the ones that I thought might knock me down and it didn't," says Hutton.

DIGITAL JOURNAL

Scan QR code or click to watch **Jennifer Hutton** and a fellow Fawn Annan Memorial Award finalist in a Digital Journal roundtable.

Thank you to our sponsors

Lenovo

ZOHO

ARMADIN

QRX | TECHNOLOGY GROUP

RED X CARBON

CIO ASSOCIATION OF CANADA

We are CIOs, CISOs and IT Leaders in Canada

7270 Woodbine Avenue, Suite 305, Markham ON L3R 4B9 | 905-752-1899 | **ciocan.ca**