FEATURE

# Protecting New Brunswick from the World Wild West

If you ask Dr. Ali Ghorbani what it takes to coordinate a strong cybersecurity effort in New Brunswick, it becomes clear he's given it a lot of thought.

"For cybersecurity efforts to work, you need all levels of government, academia and industry to work together," says the director of the Fredericton-based Canadian Institute for Cybersecurity (CIC). "Cybersecurity breaches impact us all, so it's crucial that we work together to prevent them."

Dr. Ghorbani's vision of a more cybersecure province took form in early 2007 with the creation of the Centre of Excellence in Cybersecurity on the Fredericton campus of the University of New Brunswick (UNB). "One aspect of cybersecurity that we realized needed to be addressed was its interdisciplinary nature," Ghorbani says. "It isn't just about computer science. It involves business, education, psychology, design – the list goes on."

In January 2017, UNB, the Atlantic Canada Opportunities Agency (ACOA) and the provincial government took it a step further with the creation of the CIC: a comprehensive multi-disciplinary training, research and development, and entrepreneurial unit that draws on the expertise of researchers in the social sciences, business, computer science, engineering, law and science.

The need to build a strong cybersecurity program is now a fact of life across all disciplines. Digital medical records are used to build health-care profiles; chemistry and life sciences store vast quantities of biomedical data; and the legal system generates an ever-increasing amount of sensitive information.

"Ultimately, it's people who are responsible for safeguarding the systems that contain vulnerable

# World Wild West – continued

information," Ghorbani says. "It is crucial that we safeguard New Brunswick's critical infrastructure. For instance, if a breach managed to compromise our power grid, it would be very logistically and financially painful for us."

Making New Brunswick cybersafe comes with a unique set of challenges.

"The lack of awareness among New Brunswickers is our main challenge," Ghorbani says. "Many New Brunswickers do not have the fundamental knowledge of how to stay safe in cyberspace. To address this issue we in collaboration with CyberNB made a concerted effort to go into schools and provide workshops that shares this knowledge. I'm hopeful that we'll start providing this training to seniors as well."

So when asked how can we protect ourselves, Dr. Ghorbani stated the number one thing is to practice vigilance. "Don't be too trusting in cyberspace – it's still the Wild West," he says. "Be suspicious of things that are not known to you. Make sure your systems are up-to-date with the latest operating systems and patches."

Dr. Ghorbani notes the need to tread carefully will only become greater as the level of risk intensifies – particularly as artificial intelligence and automation become more prominent.

"We've just seen the tip of the iceberg with the Internet of Things," Ghorbani says. "Artificial intelligence and machine learning, helpful as they are, bring forth a whole new set of vulnerabilities that the bad guys can exploit."

**"Ultimately, it's people who are responsible for safeguarding the systems that contain vulnerable information. It is crucial that we safeguard New Brunswick's critical infrastructure."**

**"Don't be too trusting in cyberspace – it's still the Wild West. Be suspicious of things that are not known to you."**

It has become apparent that education plays a significant part in reducing cyberrisk. UNB Faculty of Computer Science just approved a one-year Master of Applied Cybersecurity program – this in addition to the undergraduate programs offered on campus.

"Education, education, education," Ghorbani concludes. "That's the way to fight cybercrime."

The **Internet of Things** refers to the concept of connecting any device with an on and off switch to the Internet (and/or to each other). This can include cellphones, coffee makers, washing machines, headphones, lamps, and wearable devices. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig.