Highway Robbery on the Information Superhighway

In David Shipley's words, no one talked about highway robbery on the information superhighway, but unfortunately that is what's happening now.

"The internet was never designed to be secure, and in the cases of many technologies being developed today, cybersecurity is an afterthought," says the CEO of Beauceron Security Inc. "Despite these risks, many are still behaving as though better technology is the only solution to cybercrime. We're totally ignoring the human element."

A recent study from IBM concluded 95 per cent of successful cyberattacks are the result of human error – employees clicking on a link in a phishing email, for instance. These mistakes cost the victims dearly. A 2015 study by a British insurance company found that cybercrime costs businesses worldwide $400 billion a year.

The cultural problem standing in the way of cybersecure workplaces is what drives the effort at Beauceron. The business, now in its third year of operations, was named after the French sheepdog with the intention of replicating its behaviour and turning company employees into the protectors of the business' digital assets. This thinking is a radical shift in the way a company is usually protected, as most rely on their overworked team in the IT department.

> **"The internet was never designed to be secure."**

Today, Beauceron offers cybersecurity training, online teaching, phishing simulations and a suite of other services with the aim of simplifying the learning curve and changing behaviours to reflect real business vulnerabilities.

Highway Robbery on the Information Superhighway – continued

David Shipley's Tips:

Three steps anyone can take to protect their devices from hackers

1. Get informed.

You don't have to be an expert, but you do need to pay attention. Ask yourself: What devices do I have in my household? Is my software up to date? (Fun fact – The Equifax breach was a result of the company neglecting to update its servers.) At the office, ask your IT manager if your computer is up-to-date. You can help spot problems.

2. Treat cybersafety just like physical safety.

It's easy to forget that something like a weak password can make you just as vulnerable as having a $100 bill hanging out of your pocket in a crowded place.

3. Report suspicious emails or other unusual activity to your IT team.

When you report that strange email, you protect others in your organization who might get the same message – all while helping the team better understand the attack.

Shipley's prediction for the future of cybersecurity? It's going to get worse before it gets better, particularly as it relates to what he calls a massive regulatory gap.

"The example I would use is the Titanic," he says. "It was the first major marine disaster to prompt the creation of stronger regulation for marine safety, including the required number of lifeboats aboard each ship.

"The *Digital Privacy Act* is going to need a similar upgrade," he continues. "Right now the maximum fine for a breach is $100,000, which is a blip on the radar compared to how much money hackers can steal."

What's more, the struggle to catch hackers in the act won't get any easier. In Canada, suspects are only ever identified in six per cent of police-reported cybercrimes.

"Right now the maximum fine for a breach is $100,000, which is a blip on the radar compared to how much money hackers can steal."

Shipley stresses that not all hope is lost. Cybersecurity is in the hands of people who can take concrete steps to protect themselves and their workplaces.

"When individuals are given the right tools and education, empowered to understand their role in protecting an organization and encouraged to do so, they're energized by the idea of playing their part," Shipley says.