HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

# Standing Committee on Public Safety and National Security

SECU • NUMBER 147 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

## Monday, February 4, 2019

## Chair

**The Honourable John McKay**

# Standing Committee on Public Safety and National Security

**Monday, February 4, 2019**

● (1530)

[*English*]

**The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)):** I call the meeting to order.

We have with us Jobert Abma, founder of HackerOne; Deborah Chang, also from HackerOne; and as an individual, Steve Waterhouse.

I'm sure that you have been briefed by the committee as to the process. It's 10 minutes for the initial presentation, and then we'll go to Mr. Waterhouse for his 10-minute presentation, and thereafter to questions by members.

Our second hour has collapsed, so I intend to run over our time, assuming that our guests will continue to be available.

With that, I will turn to HackerOne.

**Ms. Deborah Chang (Vice-President, Policy, HackerOne):** Members of the House of Commons Standing Committee on Public Safety and National Security, thank you for inviting us to speak today. I look forward to providing you with our perspective on cybersecurity and bug bounty programs.

I am vice-president of business development and policy of San Francisco-based HackerOne, the world's leading provider of hacker-powered security. I'm here with Jobert Abma, the founder of HackerOne. He founded the company when he was 23 years old and has been hacking since he was 13.

HackerOne operates bug bounty programs that connect companies and governments with the best white hat hackers in the world to find and fix vulnerabilities before malicious actors exploit them. As of January 2019, over 300,000 white hat hackers have registered with HackerOne to defend customers,—among them, the United States Department of Defense—removing over 80,000 vulnerabilities and preventing an untold number of breaches in the process.

Today's cybersecurity practices are severely outdated, in contrast to the cyber threats that society faces. When exploited for criminal purposes, even just a single and relatively unremarkable security vulnerability can create havoc, as the Equifax data breach grossly reminded us in 2017. In 2018 many other breaches have made the press, including the WannaCry ransomware attack.

For financial institutions, fraud incidents both online and offline increased by more than 130% in 2018, resulting in significant monetary and reputational losses. In the U.K., the number of cyber-attacks against U.K. financial services reported to the U.K.'s Financial Conduct Authority has risen by more than 80% in the last year. It is an unfortunate fact that in the digital realm, society is currently failing to provide its citizens with what societies were established for: safety and security.

I would like to talk now about hacker-powered security—a scalable model that can be used to prevent cyber-attacks in society as a whole, especially in the financial industry and national security. Whatever protections and defences we build into our digital assets—and we should build a lot of them—there's one practice that covers every possible cause of cyber breach. There is an immune system that will approach the digital assets from the same direction as adversaries and criminals, from the outside. There is a mechanism that, at scale, has the opportunity to ultimately detect every hole, every weakness and every security vulnerability in a system or product built by humans.

This practice is often called hacker-powered security. Hacker-powered security covers any cybersecurity-enhancing services and automations that are partially or wholly produced by independently operating security experts outside the company or organization in question. It is a model that invites external and independent security researchers and ethical hackers to hunt for vulnerabilities in computerized systems. These are individual experts who have signed up to help corporations and organizations detect and fix their security weaknesses.

The most fundamental function of hacker-powered security is a vulnerability disclosure program, also called responsible disclosure or coordinated vulnerability disclosure. A vulnerability disclosure program is essentially a neighbourhood watch for software. The motto is “If you see something, say something.” Concretely, if and when an ethical hacker finds a security vulnerability in a company or government organization's website, mobile app, or other computer system, this person will be invited to disclose to the system's owner the vulnerability that was found.

Most human beings are ready to help their neighbour, so the impetus for vulnerability disclosure is enormous. Issues of legality and trust, however, make vulnerability disclosure more complicated than a regular neighbourhood watch. To solve this issue, leading companies have created their own policy frameworks for the disclosure of vulnerabilities to them, and others turn to companies such as HackerOne to organize and coordinate such programs.

When an entity decides to offer financial rewards to finders of vulnerabilities, the vulnerability disclosure program is called a bug bounty program. Bug bounty programs have existed since at least 1983. The practice was perfected by Google, Facebook and Microsoft over the past half-dozen years.

● (1535)

Hacker-powered security programs have demonstrated their effectiveness compared with other methods of vulnerability detection. Hiring full-time employees or external service or product vendors to test for vulnerabilities is more expensive. No other method for validating software or manufactured products in use by consumers has been shown to produce similar results at such a favourable economic unit price.

Hacker-powered security is a scaled model. Today, there are over 300,000 registered ethical hackers on our platform alone, and over the coming years, we hope that this number will grow to over one million. The army of hackers will be able to take on the work of the entire digital realm of our society.

Thanks to the diversity and scale of the hacker community, hacker-powered security finds vulnerabilities that automated scanners or permanent penetration testing teams do not. Existing models are good at finding predictable security vulnerabilities, but even more important is to find the unpredictable ones: the unknown unknowns. Given a large enough hacker community and enough time, such vulnerabilities will be identified.

Entities that operate such vulnerability disclosure or bug bounty programs include Adobe, AT&T, the U.S. Department of Defense, Dropbox, Facebook, General Motors, Google, Microsoft, Nintendo, Starbucks, Shopify, Twitter and United Airlines. Specifically in the financial industry, American Express, Citigroup, JPMorgan Chase, ING and TD Ameritrade have public VDPs.

The U.S. Department of Defense and HackerOne pioneered the first federal government bug bounty program. Since the program's inception, more than 5,000 security vulnerabilities have been safely resolved in DOD critical assets with hacker-powered security. While the majority of the vulnerabilities reported through the DOD were without financial compensation, hackers have been awarded hundreds of thousands of dollars in bug bounty payments by the DOD.

A question I get a lot is, who are these hackers? Security experts may be described using a variety of titles, including ethical hacker, white hat, security researcher, bug hunter and finder. One title is conspicuously absent: criminal. Hackers are not criminals. Specifically, bug bounty programs offer no benefit to someone with criminal intent. On the contrary, HackerOne will record data about every hacker on the platform and only reward action that followed the rules. For these reasons, criminals go elsewhere.

Hackers are driven by a variety of motivations, many of which are altruistic. The security advocacy organization I Am The Cavalry summarizes these motivations as to protect—make the world a safer place; puzzle—tinker out of curiosity; prestige—seek pride and notability; profit—to earn money; and protest or patriotism—ideological and principled. A 2016 study by the U.S. National Telecommunications and Information Administration within the Department of Commerce found that only 15% of security researchers expect financial compensation in response to vulnerability disclosure.

Hacker-powered security not only improves security, but the model democratizes opportunity and offers meaningful work to anyone with the inclination and drive to be a useful, ethical hacker. Many hackers are young adults. They can do their work from anywhere. The money hackers make is used to support families, pay for education and catapult them into successful professional careers.

Hacking brings meaning and mandate to enterprising people irrespective of their location. Hacking brings positive societal impact across the nation.

In conclusion, we need hackers. Our goal must be an Internet that enables privacy and protects consumers. This is not achievable without ethical hackers taking an active role in safeguarding our collective security. Hackers are truly the immune system of the Internet. They are a positive power in society. We must enable them to encourage contribution. This requires a safe legal environment, encouraging all individuals to come forward with vulnerability information, no matter what the circumstance.

● (1540)

To close, I will repeat the words of numerous experts that a ubiquitous “see something, say something” practice for vulnerabilities is a vital and critical step towards improving cybersecurity for consumers. The absence of a formal channel to receive vulnerability reports reduces a vendor's security posture and introduces unnecessary risk. Corporations and the government should welcome input from external parties regarding potential security vulnerability. The Canadian government should encourage, if not require, that behaviour.

Thank you for the opportunity to testify on this important issue.

**The Chair:** Thank you very much.

With that, we'll turn to Mr. Waterhouse.

**Mr. Steve Waterhouse (Former Information Systems Security Officer, Department of National Defence, As an Individual):** Thank you to the committee for the invitation to share insights on some of the problematics perceived by fellow citizens with their access and/or security of their earnings or savings versus computer technologies.

First, I will give you a brief introduction of where I come from. After serving with the Canadian Armed Forces and DND for 23 years, I was privileged to be among the first cyber-soldiers in the country to manage networked information systems, from a LAN size of about 250 users to a MAN size of about 5,000 users on multi-sites at a base level in its early stages of integration. This was in order to provide the right information to the command structure in what was previously a paper-based process, from normal day-to-day office tasks to the academic activities I was doing at CMR Saint-Jean as well as in operations. More recently, my job has been educating and training professionals and the public on how to apply best practices in information technology and to explain, in plain language—as we will do today—what is happening in the cyber space that affects everyone and everything on almost a daily basis with the news media. I shall present these insights to you now.

[*Translation*]

The situation is that it is a quarter past midnight.

This is the 21st century, as you all know. We are more connected than ever and our lives are more and more automated. In large part, the country's economy depends on the use of technology, by small and medium-sized companies and by big business. Even government services have turned a technological corner. The reality, however, is catching up with us more and more.

The few examples listed in the document I submitted to the committee demonstrate that the problems will continue as time goes on, but they are still of concern now. For example, the smartest programmers and IT experts are designing improper configurations in order to give themselves an unfair advantage in their stock market transactions.

Anyone who takes the time to learn about using, or even hacking, technology can find on the Internet techniques to find loopholes and to get around security, The latest techniques can be used to exploit the flaws, most of the time in order to get one's hands on information that will lead to financial gain.

In recent years, especially in 2017 and 2018, we have heard that ransomware is pervasive and virulent. It can attack not only individuals, but also any organization at all without exception. This type of scam still affects us because people are poorly informed and unable to identify the threats. The wrongdoers, moreover, have refined their methods, so that it is more and more difficult to identify the malware in a real email message.

Today, financial institutions are asking, not to say demanding, that their clients conduct their financial transactions only from their personal computers, their mobile phones, or by some other connected means. They expect everyone, employees and customers alike, to know how to work Windows 10, or the most recent version of Microsoft Office.

People do not have the training or the knowledge to use the basic tools used in those transactions. Most of the time, the transactions are conducted when security measures are not the best and the connectivity is dubious. Public Wi-Fi connections in hotels or Internet cafés are not secure at all. Cell phones, while they are hacked into less, are just as lacking in security.

The delay in deploying the promised high-speed connectivity to our regions reinforces the cynicism that come from the lack of access to a speed decent enough to allow financial transactions. The cynicism come from the fact that businesses and residence in Port-au-Prince, Haiti, have or, in the coming years will have, access to fibreoptics, well before those only 50 kilometres from Montreal.

● (1545)

[*English*]

What should we do, or what can be done? Well, I say take the lead and lead by example. It was with much enthusiasm that I heard about the set-up of the Canadian Centre for Cyber Security last October. This distinction of “cyber” as a separate component of “security” needed to be on its own to underline its importance. Too often I have encountered in large enterprises, as well as SMBs, “computer security” being considered as under the responsibility of the first appointed volunteer in the room. It's a necessary evil to many, but by having the federal government proceeding this way, few reasons can be found by any enterprises to set aside matters of cybersecurity and, hence, put the matters front and centre.

The CCC's recent changes in resources devoted to cybersecurity were long overdue. Canada used to be the nation of telecommunications firsts. Now we are dragging behind the rest of the world; we are trying to keep up with a technological wave of innovations. We used to have the best telecommunications equipment maker in the world called Nortel. It was taken away from us. Canada was one of the first nations to stand up as a leader in quantum security for computer networks. Most of that research was taken from us recently.

Strengthening the government's information systems has helped greatly to ensure their availability. Everyone can consult their information at any given time. As you have come to know, the prime target in computer exploitation is the weakest link, which to this day is the human component, particularly for the average citizen, whether at home or on the road.

The emphasis is on having a strong economy while using IT. This can be achieved by using information technology and by taking a live rather than a computer-based approach to educating those who use that technology. That means pretty much everyone nowadays. This approach reassures and gives the citizen or user immediate feedback.

Every day, Mr. and Mrs. Everyone are using incomplete software and hardware brought to this market without any guarantees that it will work—or that it won't fail. When cars are sold in this country, they come with all sorts of seals of approval, and Transport Canada oversees their safety. You can buy a set of Christmas lights anywhere in the country and they will come with a seal of approval from the CSA. Industry Canada oversees their application and safety. Who applies the same controls and validation to computer code or electronic hardware?

These devices on which we depend each day—also known as IoTs—are roaming freely all around us, without any form of safety certification. Insulin pumps are an example. Although the importation and sale of such devices seems to be regulated by Health Canada, who oversees the code used by these devices to keep people alive? Are they doing the right thing? Are pacemakers in the same situation? I believe they are.

Who certifies the computer code for ATMs to ensure that Canadian citizens have access to their money when needed, or smart dolls? We hear that they are being sold in North America even though they have been declared illegal spying devices in Germany due to privacy issues with kids. Who is supposed to protect our children's privacy from these immoral devices, if not the Privacy Commissioner?

Hardware and software code should be overseen by an independent government agency like CSA, as an example. Ideally, this agency would have a say about what's distributed for life-critical devices and would impose stiff penalties for non-conforming products—or simply ban them from the market.

In that matter, we are now confronted with a new dynamic in today's economy, the use of biometrics to do business. In July last year, the Chinook Centre in Calgary was caught embedding facial recognition cameras in the mall's interactive panels. It was documenting the clientele without their knowledge, with no warning whatsoever.

Complaints were made to the privacy commissioners of Canada and Alberta. To this date, none of the reports from these investigations, started in August 2018, have been published. I just came from the Promenades Gatineau, where I documented the presence of these panels, though not from the same company. They embed cameras on the panels without warning people they are being documented at that place.

We are now confronted with a similar situation at Place Laurier, where four stores are openly using facial recognition with the goal of documenting clients' feedback through their biometric characteristics. This kind of tracking is already happening with cellphones, of course, and the *fidélité* cards that consumers use in stores.

It would certainly be beneficial to everyone if the OPC were to grant authorizations, after a proper accreditation process, to organizations and businesses for the use of biometric technology. This would minimize the cost overruns of inquiries and also reassure citizens that the government has their backs with respect to privacy matters.

● (1550)

[*Translation*]

Is it too late? No, I believe that there is still time to do things right.

As for any tool, we must take the time to read the manual before we use it. Who among you has used or read the manual for Windows 10, Windows 7 or Windows XP? My feeling is that none of you did. They are very large documents. People are afraid of them and run a mile. At that point, third-party assistance becomes necessary. The human beings using the machines still need other human beings to train and guide them.

Your enlightened study of this issue will certainly be appreciated and will allow for improvements to what is not working well. That will create the impetus we need for the various participants to contribute to a better economy and it will help us once more to become the leaders that, fundamentally, we are.

[*English*]

I am now available to answer questions in both official languages.

Thank you.

**The Chair:** Thank you, Mr. Waterhouse, Ms. Chang and Mr. Abma.

Our first questioner is Ms. Dabrusin.

Take seven minutes, please.

**Ms. Julie Dabrusin (Toronto—Danforth, Lib.):** Thank you.

There is a repeating theme from last week. I was really struck by the evidence we heard last week. The financial institution was described as the armoured vehicle delivering between two cardboard boxes, which are the humans at either end. I believe the number we heard was that something like 60% of cybersecurity issues are human-created by the end-users. That's something that really stuck out.

You asked whether we are reading the manuals. I don't think we are reading all of the manuals, and I don't know that it's reasonable to expect that we should.

You've mentioned government certification for end-users as one part, but another big piece is education.

HackerOne, I was looking at one of your newsletters. You had something about phishing, a phishing quiz. It was really hard.

My question is, if you had three things, say, that you would suggest, if we were trying to properly educate people—because that seems to be one of our biggest issues—what would they be?

Let me start with you, Mr. Waterhouse.

**Mr. Steve Waterhouse:** Throughout the country I've done some training. I do many conferences on cybersecurity. As I teach professionally, I can tell you, the utmost necessity is to have people stop and take the time to read about whatever they're doing.

We're laughing about the fact that we never read any manuals. That's true, but they're often superseded by statements of legal liabilities and obligations that discourage anyone from reading beyond that point. People will just figure it out. The graphical user interface has been so successful that people just intuitively make their way through and use maybe five or ten per cent of the full capacity of software.

I saw that transition when secretaries moved from WordPerfect 5.2 to Microsoft Word. They had to take courses, because those were two separate kinds of software. They were masters at WordPerfect, while nobody was afterwards in Word.

**Ms. Julie Dabrusin:** You're telling us, then, to read the manuals.

**Mr. Steve Waterhouse:** They could not read the manual, because it was so complicated. It was such a complete package, it would have been a week-long course. They went to those week-long courses, but they were divided into three different levels of difficulty: beginner, advanced, and then expert level. These were secretaries who were at the expert level on one software. Now the new software comes around, and they are at the beginner level. That reduces the efficiency of the workforce and slows down the effectiveness of the economy, I say.

Let's say that Windows version 15 is around the corner next year. How many people will be able to know how it works? The adaptation curve has been very steep.

**Ms. Julie Dabrusin:** I'm going to go to HackerOne quickly. The phishing quiz there was a Google-something quiz, but it was hard.

Do you have any idea—simple things...? People don't want to be a cardboard box.

**Mr. Jobert Abma (Founder, HackerOne):** I would like to point out that in recent years the behaviour of consumers has changed radically. Up until five years ago, our data used to be at large organizations who would have large teams who would help us consumers protect against data breaches and protect our privacy. I think consumer behaviour has changed such that we have become responsible for our own privacy, and as Mr. Waterhouse pointed out, we do not take responsibility to the point that is necessary today.

What I would like to add is that I don't believe it is up to the consumer to guarantee their own privacy. I believe that the organizations should help consumers and help organizations to protect consumers and their own users from these data breaches.

As I said earlier, however, with those users now being responsible themselves, it is important that we do quizzes such as the phishing test you were referring to, to make people aware of some of the risks that happen when they store their data either in a certain system or with a certain organization. That is a problem that we need to address from both the consumer side as well as the standpoint of the organizations that have a copy of that data.

● (1555)

**Ms. Julie Dabrusin:** Let me stay with your group. One thing you talked about was the importance of being able to report vulnerabilities, of a hacker who finds a vulnerability being able to report it. You mentioned that there was an issue with the legality of this.

Is the legal challenge that they will be charged criminally? What would we need as legal protection for the hackers doing good?

**Ms. Deborah Chang:** That's a great question. In the U.S., there is the Computer Fraud and Abuse Act, passed in the 1980s, that says something to the effect that you can't hack and enter into a company's digital assets in an unauthorized manner. It has not been updated since. I believe Canada has a version of that law as well.

We would encourage Canada to pass a law to encourage all organizations with a digital asset to adapt some form of policy to invite the public—and you don't even need to call them hackers—to report any bugs and vulnerabilities they happen to find. That is just inviting them in, saying what's in scope and what is permitted and what isn't, as well as what you might specifically be looking for. Then, importantly, the organizations should offer a communication channel within it and set up a process in which to receive that information, as well as the resources to fix it.

That's what we would generally encourage the government to do, to pass a law to encourage that type of behaviour.

**Ms. Julie Dabrusin:** I have 20 seconds.

You tell this one company, you found a bug, a deficiency or vulnerability. Then you might have a whole bunch of companies using exactly the same type of software or whatever. They have the same vulnerability. What do we need to do to be able to share that vulnerability information across different businesses or organizations?

**The Chair:** Be very brief, please.

**Mr. Jobert Abma:** There's a process called vulnerability coordination, where you would work together with the vendors themselves to coordinate that vulnerability, to disclose it to other organizations using the same vulnerability.

**The Chair:** Thank you, Ms. Dabrusin.

[*Translation*]

Mr. Paul-Hus, the floor is yours for seven minutes.

**Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC):** Thank you, Mr. Chair.

Good afternoon, everyone. My first question goes to Mr. Abma.

Last September, Scott Jones, the director designate of the Canadian Centre for Cyber Security, told our committee that he was convinced that Canada had sufficient guarantees to allow us to address the dangers of Chinese hacking or espionage of our telecommunications. In his statement, Mr. Jones concluded that it was not necessary to follow our allies in the Five Eyes to keep one company out of our 5G networks.

Can you talk to us about the strength of our cyberspace in Canada?

[*English*]

**Mr. Jobert Abma:** There has yet to be a government that is immune to cybersecurity threats. The U.S. has some of the most developed cyber-practices in the world, as does Canada, as Mr. Waterhouse pointed out. It is also home to the companies with the most mature security practices in the world. Even so, hacks may still happen. So we're up against a race.

The Internet is a very complex system with a lot of people contributing to it. Everything is tied together. Systems and networks change or contain hundreds of thousands of individual hardware and software components and thousands of lines of code. Every time code is updated, which may happen multiple times a day, new vulnerabilities may be introduced. There will always be unknown unknowns and the only way to uncover these unknown unknowns is to invite good hackers to test the system. Even with systems that have been proven to be very secure, changes may happen overnight either because of an internal or external change, and vulnerabilities may arise.

● (1600)

[*Translation*]

**Mr. Pierre Paul-Hus:** Could you tell me whether, in America, your teams and your hackers are ready to handle the dangers besetting the 5G networks?

[*English*]

**Mr. Jobert Abma:** Good hackers come across new technology every day. They will have to familiarize themselves with new technology to be able to find security vulnerabilities in it or in the components that are built on top of technologies like 5G. With our diverse customer base, there are a lot of opportunities and incentives for the hacker community to dive into these new technologies. As 5G becomes mainstream, we believe that more people will be capable of auditing the security of such components.

At this time, multiple customers of HackerOne are launching components on top of 5G and are exposing that technology to some in the hacker community, which we believe is the right way to uncover some of these security vulnerabilities that are currently unknown to us or the United States.

[*Translation*]

**Mr. Pierre Paul-Hus:** Your company, HackerOne, has established relationships with clients like the Pentagon and the American Department of State. How have you managed to establish a relationship of trust with those clients, and how could we do the same? Is this a practice that Canada should adopt?

[*English*]

**Mr. Jobert Abma:** All the hackers who have participated in the DOD-related programs were hand-selected by the DOD and HackerOne because of our expertise and track record. We complement what our customers and government are already doing. We have a proven track record in hacker-powered security, and having coverage in both the government and private sectors strengthens our mission, which is to empower the world to build a safer Internet.

To this day, over 5,000 vulnerabilities have been uncovered in the U.S. DOD systems, the majority of which have been reported to the DOD without any monetary incentives. We believe that a vulnerability disclosure program, or establishing a process to do so, is our recommendation to every government on this planet to ensure that they can work with the hacker community according to the “see something, say something” principle.

[*Translation*]

**Mr. Pierre Paul-Hus:** Thank you. If the committee is interested, I have a photo of your brochure showing hackers working for the Department of Defence. They do not want to put on a uniform, but they are the best.

Now I have a question for you, Mr. Waterhouse. Are financial institutions currently doing enough to protect people on a daily basis?

**Mr. Steve Waterhouse:** The financial institutions say yes. From my point of view as a customer of a financial institution, I say no. Often, customers go to their financial institutions, where they are given tools that the institutions guarantee are secure. The clients go home or to work with a tool, an application, to access the system, but they really do not know how it works. All the risk then falls on their shoulders. If they make a mistake, it's their fault, not the fault of the financial institution, which has no problem proving it.

That is the shame. I was somewhat preaching the need to know one's operating system. Will the next Andoid phone be up to the task? People will not know how to use it any better. The training will focus on one application only and people will have to adapt when the application changes its look and its feel. This is what the market has been forcing on us for 30 or so years. As soon as the look and feel of an application changes, you have to work at adapting to it. There is no update, and no one holds our hand to help us become familiar with the new application.

● (1605)

**Mr. Pierre Paul-Hus:** Right.

[*English*]

**The Chair:** You have 20 seconds left.

[*Translation*]

**Mr. Pierre Paul-Hus:** What is the best way to make people aware?

**Mr. Steve Waterhouse:** Financial institutions should invest a little more in training people, their customers. Training sessions should not be by means of videos on the Internet, where it is easy to become distracted.

The training should be interactive so that we know whether the customers have fully understood. When training is done on screen, especially after some time, a customer can push the “pause” button and start again, which is great. If not, the customer can also decide to press the “play” button and go and do something else in the meantime. You never know whether they have understood the information. The box will be checked off, but you will never know whether the material has been absorbed properly.

**The Chair:** Thank you, Mr. Paul-Hus.

Mr. Dubé, you have seven minutes.

**Mr. Matthew Dubé (Beloeil—Chambly, NDP):** Thank you, Mr. Chair.

[*English*]

I want to ask a question of the folks from HackerOne, since the example I will use is what's going on currently in the U.S.

The NSA does what they call a vulnerabilities equities process, or VEP. Probably about a year ago I was asked about this by a journalist, because our equivalent body here—not quite equivalent; it's not always exactly analogous—the CSE, doesn't have the same kind of transparent process.

I wonder if you could talk about whether that process—in your mind, given the work that you do—has been successful in achieving more transparency when the agencies themselves are discovering vulnerabilities in software that they could potentially use to glean all kinds of information on people?

**Mr. Jobert Abma:** Yes, I'd be happy to take that.

The U.S. government has spent a lot of money and time in securing its own systems. Our data shows that after it established a transparent process to work with the hacker community, over 5,000 security vulnerabilities were identified, for which hundreds of thousands of dollars have been awarded as an additional incentive to those hackers to look into those systems.

The number of vulnerabilities discovered by the hacker community is much greater in volume than some of the vulnerabilities identified by the U.S. government itself. The fact that there are so many of them shows that working with hacker communities is the right thing to do to uncover more security vulnerabilities.

**Mr. Matthew Dubé:** That's an interesting point, because it leads me to another question of mine, but let me back up for a minute. If law enforcement wants to unlock, say, an iPhone to obtain information that's on it, there's obviously a process in place to do so with obtaining a warrant. Obviously, it might vary in both our countries, but I think the spirit of it is similar enough that we can discuss it. My question then becomes this. If a hacker wants to do good, let's say, as a white hat hacker, the hacker might look to the government thinking that they are doing the right thing by providing that information, but it doesn't necessarily then go back to the company, and people remain vulnerable because that agency might have an interest in keeping that vulnerability. Do you think there should be some kind of law or regulation in place that creates the same kinds of checks and balances on the police when they obtain a warrant to unlock a phone and apply those checks and balances to national security agencies as well? They would say that if you want to use a vulnerability, then you have to go through the same hoops required of law enforcement to protect people's privacy.

**Mr. Jobert Abma:** It is an ethical dilemma that I think is very important to cover. The problem that we've seen so far is with governments buying zero-day vulnerabilities, meaning vulnerabilities that are not known to the vendor who is there to patch them. These are currently being used in warfare to extract information or intelligence that is currently unknown to them. By not disclosing that to the vendor, you're also putting your consumers or citizens at risk by not disclosing that.

We believe that zero-day vulnerabilities should be reported to the vendor no matter what, but we're addressing that from a different side. We're addressing that by leveraging the hacker community to find the same vulnerabilities that either their government or criminals have found, which will then be disclosed to the vendor directly. That is our way of making sure that those vulnerabilities are becoming known to the vendor.

It would be amazing, in my opinion, if the government would also have a law like that, because I don't believe it is worth the risk for your own citizens. However, I think we're far away from having that today.

● (1610)

**Mr. Matthew Dubé:** I appreciate that response.

[*Translation*]

My final question goes to you as well, Mr. Waterhouse.

[*English*]

This is the question of the role of media essentially and the fact that some of these vulnerabilities get reported on. One example jumped to mind. I don't recall if I saw this in the news coverage or if someone just told me this anecdotally, so I could be wrong, but last week, when the vulnerability with FaceTime on iPhones and iPads was found, the individual who had unintentionally found the vulnerability was then asked by Apple to go through their process almost as if the person were going for the bug bounty without being a hacker. I'm just wondering about the cases were some of these vulnerabilities get found by accident and reported in the media. What impact does that have on how things play out both for the vulnerability itself and also for the effort to try to fix it afterwards?

[*Translation*]

Mr. Waterhouse, you can comment on that.

[*English*]

**Mr. Steve Waterhouse:** It's something that will be ongoing for the rest of our lives. Software is so incomplete. We have billions of lines of code right now in all kinds of applications, especially operating systems, that it's almost virtually impossible to.... Because the competition is very strong in the market, the companies just push out the software incomplete as it is and they just say they'll fix it as we go. This is one of the reasons we're getting these kinds of findings once in a while.

By an engineering analysis, people back at the company would say, well, nobody will think about doing that. But guess what? In the real world, we have people who are just doing whatever they seem interested in finding out. And, yes, by accident, they find these vulnerabilities, as we call them today. Should they be disclosed mandatorily? Of course.

The youngster and his parents went on to disclose it, and lawfully. They didn't want to exploit the situation; they just wanted to report it, and they even got turned down by the company.

Certainly I agree with you on this. There should be a law that says to a company that whenever someone comes to them, listen to that person, or whoever the party is who is bringing you the information, and act upon it promptly. If not, the company should be fined.

**Mr. Matthew Dubé:** I think I have about 30 seconds left if you guys want to jump in there.

**Ms. Deborah Chang:** I'd like to jump in. I think that fundamental to this discussion is privacy.

When I read about that situation.... Privacy, in our opinion, is a fundamental right, and your data is a fundamental right. A company should be strongly encouraged to protect one's right. In that case, I think the mom contacted Apple a couple of times. She was protecting her right, her son's right and her family's right. Not to have a VDP or a way to handle these issues infringes on one's privacy rights.

[*Translation*]

**The Chair:** Thank you, Mr. Dubé.

Mr. Picard, you have the floor for seven minutes.

[*English*]

**Mr. Michel Picard (Montarville, Lib.):** HackerOne, when you submit your report on vulnerabilities to financial service providers, what kind of feedback do you get from your recommendations? Do they implement them right away, or do they evaluate the cost of implementation versus the cost of taking the risk not to?

**Mr. Jobert Abma:** At the end of the day, a mature security organization is an organization in which every risk or vulnerability that is uncovered, regardless of its source, should be given the investment that would be needed protect the organization from the reported threat.

We've seen many organizations, including financial organizations, that have put in different defences based on the vulnerabilities that have been reported to them, in order to eradicate entire vulnerability classes or to protect consumers against security threats. Two-factor authentication is often used when you sign into a bank account.

The most common security vulnerabilities are usually pretty straightforward for companies to address, but especially with the data we have, we can help an organization to prioritize in-depth defences in order to better protect the organization in the long term.

● (1615)

[*Translation*]

**Mr. Michel Picard:** Mr. Waterhouse, on the subject of the products that financial services use, I would like to know whether their reported vulnerabilities are at the beginner level, unimportant in a practical sense, or whether the programs are now so sophisticated that, despite everything, the vulnerabilities still require an extremely high level of precision or expertise.

Where are we at the moment?

**Mr. Steve Waterhouse:** Mr. Picard, we see both extremes. Last week, for example, the personal information of 500 million customers of the biggest bank in India were exposed to the general public because the server that contained that information was not secure and had no password. A system within that megabank's network was vulnerable, plain and simple. It was a basic error; personally, I would call it a rookie mistake.

Today, Canadian financial institutions use the best equipment they can find. They have sufficient resources to afford it. The fact remains that these are commercial products, available to any company in the world and with the same kinds of vulnerabilities. So they need teams that are able to conduct checks and more checks, over and over again, in a constant cycle, in order to determine whether the system is still solid and valid. Most SMEs have systems installed for them; they say they have a firewall, they believe they are protected and they stop worrying. Unfortunately, some of that equipment is vulnerable. So the checking must be constant.

[*English*]

**Mr. Michel Picard:** In terms of strategy, as a financial service provider I may choose to split my data as much as possible to complicate things if I want to put data together to create some intelligence out of that. Or, if I go to a concept of open banking, I can centralize everything on one server for performance and efficiency. What seems to be a good strategy? We have both strategies on the table to discuss these days.

**Mr. Jobert Abma:** One of the problems we've seen, especially with some of the more recent data breaches, is that centralization of data is becoming a problem. It makes it easier for the organization to protect itself against certain risks because it is only one component that they have to defend. The problem is that when things do go wrong, through either a misconfiguration on the organization's side as happened in India, or negligence or vulnerability in third party software, the consequences are usually too big to oversee. Decentralization on the other hand is much harder to maintain. There are a lot more moving components, but from a data privacy perspective, it does look like the right way to go, the right strategy to take.

When you're talking about the insights that can be gained when it is a central system, the same thing can be achieved with multiple systems, with decentralized systems, but instead of using the data themselves, extrapolate the data or the insights away from that data and use only that to give recommendations or do the data analysis that is required. With that, a lot of organizations are moving to the cloud, which is essentially the same problem that large organizations face since they have centralized a lot of their data. We are seeing an uptick in the number of breaches that happen because people are unaware of some of the consequences of putting data into a system that they don't fully understand. This also goes back to Mr. Waterhouse's point that consumers don't read the manuals, but sometimes organizations also don't understand the threat that they're putting themselves up against by moving into new territory.

**Mr. Michel Picard:** I have just one minute left.

[*Translation*]

We have software that is vulnerable and we are beginning to look at the use of artificial intelligence to help us monitor what that software does not do well.

Should we put our trust in a system blindly? Artificial intelligence is still programmed by humans.

**Mr. Steve Waterhouse:** The situation is the same for today's software, Mr. Picard. Programmers produce operating systems that are incomplete to which we attach information-processing software that is itself incomplete.

You are asking me whether artificial intelligence will be better. I have been told that supposedly cutting-edge security measures to prevent that kind of behaviour does exist. However, I do not believe that the new software will be free from all flaws.

● (1620)

[*English*]

**Mr. Michel Picard:** Do you have a final word on that, HackerOne?

**Mr. Jobert Abma:** Artificial intelligence, in my opinion, is a very important technology that we should leverage as much as possible. At the end of the day, we believe that where people work, people will make mistakes. Artificial intelligence is not going to help protect us against these threats. Where artificial intelligence can be used to come up with defences to protect us better, we believe that is the right thing to do, but it is not a permanent fix or permanent solution to protect oneself against security threats.

**The Chair:** Thank you, Monsieur Picard.

Mr. Motz, go ahead for five minutes.

Oh, hang on, there's some confusion here.

Mr. Paul-Hus.

[*Translation*]

**Mr. Pierre Paul-Hus:** Thank you, Mr. Chair.

I want to thank our guests for being here. However, I would like to take a little time to deal with the current situation in the Standing Committee on Citizenship and Immigration. My colleague has just submitted a motion. So I would like…

[*English*]

**The Chair:** Excuse me a second, Mr. Paul-Hus. Can this be done at the end of the meeting?

[*Translation*]

**Mr. Pierre Paul-Hus:** I will be quick, Mr. Chair.

[*English*]

**The Chair:** There's no such thing as a rapid motion.

[*Translation*]

**Mr. Pierre Paul-Hus:** I will read my motion quickly and the committee can decide.

[*English*]

**The Chair:** Okay. Personally I'd prefer it to be done at the end of the meeting, but if you insist on going forward, I have to take it out of your time, which is regrettable because I love Mr. Motz's questions. Okay.

[*Translation*]

**Mr. Pierre Paul-Hus:** That is what I would have preferred too, but I may not be available at 4:30 p.m. So I will continue, Mr. Chair. I apologize.

I will read my motion for the benefit of my colleagues:

> That, pursuant to Standing Orders 108(1)(a) and 108(2), the Committee meet jointly with the Standing Committee on Citizenship and Immigration to study whether gaps in the process of the security screening for persons entering Canada have arisen over the last three years, both at official points of entry and between points of entry, to identify the causes and impacts of these gaps, and propose potential solutions; that departmental officials and Ministers from both Immigration, Refugees, and Citizenship, and Public Safety and Emergency Preparedness be present for at least one meeting; that officials and elected representatives from the United States federal Congress and Senate be invited to attend; that these meetings be held before Friday, March 1, 2019; that the Committee report its findings to the House; and that pursuant to Standing Order 109, the government table a comprehensive response thereto.

[*English*]

**The Chair:** Okay.

This motion has proper notice. It's properly before the committee. I would prefer that it be done at another time, but it is what it is, and I'm assuming somebody wants to speak to it.

Ms. Damoff. Again, I apologize to the witnesses.

**Ms. Pam Damoff (Oakville North—Burlington, Lib.):** Thank you, Chair. I too apologize to the witnesses for taking up their time.

I'm disappointed, but I guess I shouldn't be surprised by this motion. It's typical of what the Harper-Scheer Conservative style of politics has become. They want Canadians to be afraid, and once again are choosing to scapegoat newcomers.

[*Translation*]

**Mr. Pierre Paul-Hus:** Mr. Chair, I would like to comment.

[*English*]

**The Chair:** Yes?

[*Translation*]

**Mr. Pierre Paul-Hus:** I simply submitted a motion according to the rules of the House of Commons. It is not appropriate for my colleague to start playing politics at this table.

[*English*]

**The Chair:** If we could minimize the partisanship on a partisan motion, the chair would be much happier.

Ms. Damoff, if you could speak to the motion, please.

**Ms. Pam Damoff:** The fact is, Chair, that Canadians can and should feel safe and secure knowing that we have a secure border and a strong screening system. Their safety has not been, and never will be, compromised. We will not be supporting this motion.

**The Chair:** Is there further debate? Seeing none, I'll call the vote.

(Motion negatived)

**The Chair:** Mr. Motz, you have two minutes left.

**Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC):** Thank you, Chair.

My first question is for HackerOne. You've basically dominated the American ethical hacker business. Do you have suggestions for best practices here in this country and how we might be able to establish that sort of reputation with the private side of ethical hacking here?

**Mr. Jobert Abma:** We believe that hacker-powered security is the key to empowering the world to build a safer Internet. Leveraging the hacker community is one of the components of a mature security organization. HackerOne leverages data to help organizations build a mature security organization and to prioritize what to work on. We encourage everybody to at least establish a vulnerability disclosure policy in order to work with the hacker community to uncover the unknown unknowns—the security vulnerabilities—in their systems.

● (1625)

**Mr. Glen Motz:** Thank you for that.

In my limited time, I want to ask Mr. Waterhouse about an electromagnetic pulse attack in Canada and the impact it would have on financial institutions. Can you talk about that for us and explain the vulnerabilities we have there?

**Mr. Steve Waterhouse:** Certainly, Mr. Motz. It's a known fact that throughout the world, we have nation-states that are actively developing such a weapon.

An EMP—an electromagnetic pulse weapon—will completely fry any electronic components, if not the electrical grid. We would go back to, let's say, how we lived in our society 100 years ago. We have had a few examples in the past. We had the Carrington event in the 1800s. We had Hydro-Québec, which was subjected to a natural EMP from the sun in 1989 that rendered the provincial power grid offline for more than eight hours.

We see ongoing developments, especially in the United States. They're forthcoming in saying that they want to have these kinds of weapons because they're not conventional kinetic weapons that can kill people. They would just neutralize the electrical environment. That said, if there's no electricity around, people will go crazy. I was witness to some of that furor with the ice storm in 1998, when for 22 or more days, nobody had access to power and to their money and so on.

Therefore, it is a direct threat to our way of life that few organizations have mitigations against, or preparation to that effect.

**The Chair:** Thank you, Mr. Waterhouse. Thank you, Mr. Motz.

Ms. Sahota.

**Ms. Ruby Sahota (Brampton North, Lib.):** Thank you.

My questions could really go to anybody.

First and foremost, I'm really fascinated by this whole bug bounty scenario. I know it's been brought up before that you're encouraging it in your testimony that organizations use this, and perhaps governments as well. I think it's been known that the Canadian government does not use bug bounties, but we do have Canadian companies that do. Shopify is one that I have read about, and there are various companies that have been using them.

I was just wondering if you could explain to me a little bit more about the trust factor, and how a company is encouraging a bounty to be put out, which means more and more hackers, whether they are good or doing the right thing, to expose their vulnerabilities to protect themselves and the information of people. How can you be sure of that? How can you verify that? When you hire an employee, you do background checks and you trust that employee because of the rapport you've built with them. These are unknown people who would be going into your systems and perhaps learning information they may have. Even HackerOne, how do you ensure that those who are hacking on your behalf are giving you all of the information they've learned, and not using it for any other cause?

**Mr. Jobert Abma:** I can take it. Thank you for that question.

We believe there's strength in numbers, meaning there are more people on this planet who want to do good. Obviously, there are always going to be people who will have bad intentions, but HackerOne does not enable these criminals to do their work through HackerOne. If they have bad intentions, they can do that work already. The thing we're opening up here is for people who actually have good intentions to use HackerOne in order to do research for some of the reasons that my colleague Debbie mentioned earlier.

**Ms. Ruby Sahota:** I understand that. Of course, people could go ahead and pursue and get that information themselves, but through this scenario, you're essentially encouraging them to, right? You're encouraging them to go into the database of a given organization. How do you ensure the people who are working for HackerOne are credible, reliable people?

● (1630)

**Mr. Jobert Abma:** Everybody who signs up for HackerOne has to provide information. As an example, we have to collect tax information to be able to pay them. Some of our customers require background checks of these people. Similar to the U.S. DOD, we conduct these background checks all around the world to ensure the identity of people before they are even given access to certain systems. At the end of the day, most of the systems that are part of the organizations are publicly facing, which means that everybody on the Internet can already attack them.

To go back to the point that I made earlier, that if there's one person who wants to do bad, there are multiple orders of magnitudes of people who want to do good. If we give them them the same incentives as criminals have to find those vulnerabilities, we believe that even if somebody outside of HackerOne finds that vulnerability and doesn't disclose it, there are enough people to find the exact same vulnerability and report it to the vendor directly.

**Ms. Ruby Sahota:** You had talked a little bit about encouraging a law to be created that allows for people to legally be able to do this. I guess that's because you feel there are some who are discouraged by the old laws that are in place. Could you explain that a little bit more to me? What would that law look like and how would it be upheld?

**Ms. Deborah Chang:** Just to add some additional data points, we did a study of our own hacking community. One in four hackers have at one time found a vulnerability but not reported it because the company didn't have a channel to disclose it. To Jobert's point, there are definitely many people out there, one in four hackers in our own community, who wanted to do more and couldn't without a safe harbour.

We're happy to work with any office to draft any law to put in the provisions, but it would just generally given the authority for a vulnerability disclosure policy. The Hack the Department of Homeland Security Act of 2018 was just passed in January, and those requiring the DHS to have a vulnerability disclosure policy in a bug bounty pilot.... And so the language—I want to say it's about six or seven pages long—authorizes the creation of VDP in a bug bounty pilot for that agency. The Hack Your State Department Act was introduced by Congress earlier this year. So there are texts of language that are out there, but we can certainly help draft that language.

**Ms. Ruby Sahota:** Thank you.

**The Chair:** Mr. Motz, you have five minutes.

**Mr. Glen Motz:** Mr. Waterhouse, I want to get back to the question we finished with before, the electromagnetic pulse attack.

In your opinion, where do you think we stand as a country in being prepared for such an attack and for dealing with one moving forward, not only against our power grids, but against any other possible targets for this sort of attack?

**Mr. Steve Waterhouse:** I saw the transition and the preparation during the Cold War period. What I mean by that is that during the seventies and eighties, computer systems in the armed forces throughout the world were susceptible to that kind of threat. Data processing rooms were built to withstand any EMPs. As time progressed and by the end of the Cold War, it was considered too costly to proceed that way, so we went on—and by “we” I mean different companies—to buy commercially available off-the-shelf computers. This is how we became vulnerable today.

Unless you have a duly prepared room to withstand any EMPs, any system is vulnerable. The telco infrastructure is vulnerable; any cars on the road that are highly electronically enabled are vulnerable.

To that extent, Mr. Motz, we are, I'm sorry to say, doomed, if one gets out and is blasted 400 kilometres above North America. North America itself will be down and we'll be living back in the way of life of 100 years ago, getting heat from wood stoves and communicating using the smoke from their fires.

**Some hon. members:** Oh, oh!

**The Chair:** —along with pigeons.

● (1635)

**Mr. Glen Motz:** —along with pigeons, yes.

We've heard from a couple of my colleagues' questions, as well as from HackerOne's sub-comments, suggestions that we can do more to get more subject-matter experts involved in this particular industry in this country.

From your perspective, what can government do to increase our capacity to deal with this from an ethical hacker perspective?

**Mr. Steve Waterhouse:** I'm not sure I'm following your question, sir.

**Mr. Glen Motz:** We have a limited capacity, a limited number of subject-matter experts, in this country to deal with what they're doing in the United States, with the volume of ethical hackers existing there.

From your perspective, is there anything that government can do to increase our capacity?

**Mr. Steve Waterhouse:** Currently, we have agencies such as CSE and the cybersecurity centre that are beginning initiatives to foster and enable some hackfest festivals throughout the country, or conferences to that effect.

As an example, I was at the hackfest festival in Quebec City in November, which for the last 10 years has been fostered by CSE. They have a preview of what's going on with the latest and greatest hackers who are around to do the hacks through whatever technological means they have at the time. It's a pool of resources they can go to to get the best from the latest and greatest they can find. There is “Atlantic con” or Atlseccon, and there is another security conference in B.C., and others across the country. In this way, the agencies are active in figuring out what's happening on a real-time basis.

I believe that with CCC's being what it is today—I mean, it's alive —it will become more invested. That, for me, would be one positive point: having a government agency always be present in letting the community know that people are....

Minister Gould just disclosed at that hackfest festival in Quebec City that Canada wanted to have more hackers present to help the Government of Canada fend off any bad influences in the next election. That was a first. Everybody was stunned by the announcement. This was a positive point, by which the government was letting the community know that they wanted everybody to pitch in and do the best we can not to have a situation like what happened in the States.

**Mr. Glen Motz:** I have one last question and I don't know how much time I have left.

Over the years, the cost of having your own business tested for outside penetration has always been high. There has been push-back from companies saying they can't afford this. It's almost the opposite: they can't afford not to do it.

Have the prices come down? Is there, not from a price perspective, some incentive through which we can give private companies, from HackerOne's perspective—small businesses, and even our large corporate businesses—the opportunity to ensure that they are at least resistant to outside attack?

**Mr. Jobert Abma:** Before I founded HackerOne, I used to be a penetration tester. One of the reasons we started the company to begin with was that we believed we needed a scalable model that would apply to every organization on this planet, and that would also be affordable for everybody on this planet. As you pointed out, penetration testing, our consultancy, has been very expensive.

We believe that the more the company has to protect, the more they need security. Because of that, everybody on this planet should be able start their own vulnerability disclosure program. At HackerOne we have offerings that are free for open-sourced and community organizations. We have help or products available for people to establish that process for their organization, even without any incentives on the platform itself. By that, we believe we will enable every organization on this planet to improve their defences against a data breach.

**The Chair:** Thank you, Mr. Motz.

Mr. Spengemann, you have five minutes.

**Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.):** This is a perfect segue. I want to pick up where Mr. Motz left off. I think it's specifically relevant to small businesses to be mindful of the obstacles to developing good cyber-infrastructure. We have a lot of start-ups that are data-intensive, where the protection of data matters early on in the corporation's lifetime, and there's a disproportionate cost borne by those kinds of businesses versus our large banks.

Besides the U.S. and Canada, are there any other jurisdictions you could point to where partnerships have been established between companies like yourselves and the public sector to establish baseline levels of security that provide a common good for the small business community, upon which further models can then be built as the companies grow and have more specialized cybersecurity demands?

Either of you, or both, could respond.

● (1640)

**Mr. Jobert Abma:** I can share some thoughts.

The problem we've seen with small organizations is that it is always a trade-off of risks. There are checklists available, or policy documentation, around what to do as a small organization. Unfortunately, it is up to the organization to implement some of those best practices that have been established. We've seen organizations, especially smaller organizations, treat those more seriously, especially as they become, as you said, more data-intensive.

However, we have not been able to establish a checklist based on the vulnerability data that we've seen on a platform level yet, but we do expect that will happen in the next couple of years.

**Mr. Sven Spengemann:** Just to follow up before we go to Mr. Waterhouse, is there something the public sector could supply? If you had a wish list vis-à-vis the public sector, whatever jurisdiction you're operating in, what could it supply to make your job easier?

**Mr. Jobert Abma:** We would be happy to work with third parties to establish that. I don't have a more concrete answer for you right now.

**Mr. Sven Spengemann:** I'm thinking along the lines of wikinomics for baseline security for small business, or a neighbourhood watch, whatever model one wants to apply. It was already touched on in earlier dialogue.

Mr. Waterhouse, do you have thoughts on this?

**Mr. Steve Waterhouse:** Yes, sir.

Some of this documentation exists already, from the NISC in the U.S., which I can say has been projected internationally and is a good way for any business to start. That documentation has been formatted for very large enterprises as well as for SMBs.

Definitely, if an SMB is serious about protecting its data, it will go through that. However, my coming from that background of SMBs, I know that they don't have time to do that. What will be needed is really something that is a one-click-stop shop. They would just have to pay for the bare minimum and have a list of whatever mandatory verification that would be done and could be satisfactory to them. But what would that satisfaction be? Would it be for the payment card industry? Would it be satisfactory for privacy issues, and so on? There's no clear guidance by which the owner of whatever coffee shop can verify, is my business satisfactorily safe in itself and for customers, and so on, and do I offer Internet access to the customers? If so, how do I do it?

I go so many times on the road, and a bad habit of mine is to verify the security in these coffee shops. Most of the time, you find you have access to the cash register as well as the operation in the back hard drive that has all the backups in it, and access to the Internet. That's the kind of purview. These SMB owners just want to make it work, because they have so little room, and cash, to get resources.

**Mr. Sven Spengemann:** Do either of you, HackerOne or Mr. Waterhouse, have comments on the Canadian labour market with respect to folks who would provide good cybersecurity? How are we doing in terms of people going through programs and being trained, whether in the public sector, the Canadian Forces, or the private sector? Is there enough of a labour force out there for us to tap into if we're doing more in that sector as a government?

**Mr. Steve Waterhouse:** I'll start with the first question. As you saw, there are so many statistics out there to say there's a lack of cyber-expertise. As testimony to that, my calendar shows that I have a reduced number of opportunities to teach and train people in it. One reason is that the costs have been going up for a few years, but another is that the people are not committing to do that job. It's a very demanding job. You have to know a lot. You have to know so many operating systems from however long in the past, and also to be able to adapt to the newest, latest and greatest ones that are coming around.

That said, we do have universities with good programs in place to train those people. I just finished doing a microprogram in cybersecurity at the master's level with the University of Sherbrooke. We had 15 people in the class. It was an awesome program, but we had only 15 people. I would have liked to have 115, because those people were really eager. They wanted to enhance their knowledge—they're professionals in the trade—but it was one of the rare occasions they had to do so.

Back in the old days, in 2003, I was with the University of Winnipeg, and that was when the first certificate came out. But the adoption is not present. It's not as forthcoming as in many countries, where they have this in their school systems.

**The Chair:** Thank you, Mr. Spengemann.

Mr. Dubé.

● (1645)

**Mr. Matthew Dubé:** I just want to go back to the issue of the next generation of 5G networks, which are still being researched, and the metaphor that Ms. Dabrusin brought up. They are cardboard boxes that an armoured truck is driving between people, but I think they're also devices. In the last meeting we had an interesting conversation about the number of devices that are now going to be in play because of the next generation networks and the speed capability—things like robots being involved in surgery and the possibilities for agriculture with drones.

I'll start with HackerOne, then go to Mr. Waterhouse as well.

I was told that price isn't the only consideration. As the market attempts to develop affordable devices for things such as smart homes and all of the other uses you can think of, is there any concern about a race to the bottom, where security will be sacrificed? You could have the Fort Knox of networks, but ultimately, if people have crappy firmware—if you'll forgive the expression—or lousy devices, the whole thing could be for naught.

Is that a concern? How would we address it?

**Mr. Jobert Abma:** This is one of the problems we haven't figured out yet—“we” meaning the world. We are seeing that there is going to be a bigger problem in that if an organization does ship firmware that contains security vulnerabilities, at some point it might not matter, because the companies will be getting away with it.

With some of the recent changes that we are seeing, there are more consequences for an organization that is neglecting security, and I think that's a good thing. Consumers demand higher standards, especially when they buy certain products. I also believe that with some of the regulations being changed, where the government can demand that organizations comply with certain standards, it's going to be very important for us to make sure that organizations do not have a chance to ship firmware that has not been tested. That, I hope, will in effect mean that we're avoiding a race to the bottom.

**Mr. Matthew Dubé:** Just before I go to Mr. Waterhouse to hear his take on this, I'll ask if you believe that planned obsolescence has any role to play in that. We see, for example, devices no longer being compatible with new firmware.

I just wonder if we're incentivizing consumers to upgrade devices perhaps at the expense of the security of the networks they're operating on, and things such as that. You would think that updating firmware is a good thing, but on the other hand, while someone might not want to be completely disconnected, they may want to keep using older technology. It might in some ways be safer.

I don't know if I'm quite right on that or if there's concern about that.

**Ms. Deborah Chang:** There is a concern, and I think that the United States as well as the U.K. have adapted standards in the area of IoT, like a list. The U.K. has a standard of 10 things that it recommends in the IoT area, and vulnerability disclosure policies are number two.

In the U.S., the FTC, the Federal Trade Commission, has taken a very active stance in requiring certain things it sees in the development of this area, as well as the FDA with medical devices. The FDA issued a medical device safety action plan last year requiring a bunch of things, even the development life cycle or the launching of a medical device.

I think the unifying theme across all of these laws and standards is that, because everything is interoperable and connected, everyone has to be doing the same thing. I think that's the purpose of all of these policies and standards, unifying standards like NIST, in these different areas.

**Mr. Matthew Dubé:** Thank you very much.

[*Translation*]

Mr. Waterhouse, do you have any closing comments?

[*English*]

**Mr. Steve Waterhouse:** We're kind of doomed, as you put it, because there are so many devices that have literally been swamping or invading the market without any such verification that they are....

I mean, these thinks put into the hands of people in the sense that they will facilitate their lives and enhance their environment. They're selling, let's take the example of a $250 thermostat that will document your way of life nowadays, and they give that information to the company that is now Google, who owns these devices. So yes, you'll be able to remotely activate your heating in your house when you come home and program it, while at the same time it will document when you're there and when you're not.

That, for me, is something that should have been taken into consideration before authorizing these kinds of devices in the market. Most people don't even realize that this kind of device is documenting their lives as they go on. Even for the other devices that we find in cars, as an example—more and more you'll have devices running the cars—they will also be hackable at the same time, because there will still be software that's incomplete.

● (1650)

**The Chair:** Formally we are at the end of our questions, but I see that my colleagues are very keen. I hope that the witnesses will have a little bit of flexibility with respect to their times. My intention is to run to about 5 o'clock, but I'm going to take the chair's prerogative here and ask a question about cryptocurrency.

In this morning's news there was a story about a company called QuadrigaCX. It was a cryptocurrency company apparently worth about $250 million. The owner was about the same age as Mr. Abma, and he died. He had all of the passwords on his laptop. It strikes me as passingly bizarre that a $250 million company is completely locked up because nobody can open up the passwords on his laptop.

My first question is whether this is a challenge for HackerOne.

**Some hon. members:** Oh, oh!

**The Chair:** Is this, on the face of it, a massive disregard of people's security?

The second question has to do with blockchain. Even if you were able to get to the passwords, is blockchain technology such that even the skills of HackerOne or HackerOne on steroids couldn't play with the security of that technology?

I apologize for these being ill-formed questions, but this does strike me as a situation where what we're supposed to be studying, financial security, comes together with a massive technological failure. It may not turn out so badly in that no ill can come from a blockchain technology that, I think, can't be cracked. Am I right or am I wrong?

**Mr. Jobert Abma:** I am familiar with the situation. There are two problems with blockchain technology that I would like to point out.

The first is that current computers are simply not fast enough, so even if we wanted to crack some of the encryptions that are being used in blockchain technology, we simply don't have the computing power to do so. It will take many years for computing power to catch up on that.

The second problem is that I think, especially with blockchain technology, because it technology is so new, consumers have put a lot of trust in these organizations that are worth hundreds of millions of dollars, but they have no idea what kind of defences have been put in place, or if too many defences have been put in place, in which case they rely on a single person.

In a way, the technologies are great and I think that experimenting with them is the right way to explore what their applications are. However, I am not of the belief that financial implementation that has taken place to date—like Bitcoin and some of the other cryptocurrencies—is the right application of the blockchain itself.

The technology itself is very powerful and should and can be used to solve some of the problems we've seen, similar to the case in which a single person has the responsibility for $250 million of other people's money and assets.

● (1655)

**The Chair:** Does it strike you as passingly absurd that the entire access to the system should be contained in one laptop?

**Mr. Jobert Abma:** Yes. That should never be the case.

**The Chair:** Okay.

For people who trade in cryptocurrencies, if one of the cryptocurrencies is locked out—and correct me if I'm wrong—am I to assume that all of the people who trade in cryptocurrencies and who have this particular kind of cryptocurrency in their portfolio are going to be affected? So it would be much larger than simply the clients of Quadriga. Is that a correct assumption or not?

**Mr. Jobert Abma:** One of the fortunate and unfortunate effects of blockchain or cryptocurrencies is that there exists only one copy of one particular block or a coin, depending on the cryptocurrency, which means that if an organization like this does not have access to what they call “wallets” anymore, the money is essentially lost and there is no way to mathematically retrieve those wallets, let alone access them.

**The Chair:** Really?

**Mr. Glen Motz:** We should ask them to speak to the people who deal in Bitcoin.

**The Chair:** Finally, I have a question on a secondary issue. Much as what Ms. Sahota said, your organization strikes me as only as strong as its weakest link. You may have 20,000 or 30,000 hackers apparently working for HackerOne, but an individual in your organization may come across a vulnerability that is actually financially more lucrative not to disclose. How, therefore, do you protect your client base from the people you have vetted and who work for you and you trust, etc.?

**Mr. Jobert Abma:** That is a great question.

This is why I believe hacker-powered security is so powerful. If there are a lot of people who have the same incentives, we believe that there are always more people who will be able to find the same vulnerability. If one of those people, whether they're a criminal or not, decides not to disclose that security vulnerability, they run the risk of other people identifying the exact same vulnerability and disclosing it to the organization.

We've never set out to compete against the black market where, essentially, zero-day vulnerabilities have been traded, either with governments or private organizations. The bug bounty programs have definitely created a reverse incentive for these black hat hackers to go after these vulnerabilities, because the prices are essentially going up simply because the chances of people with good intentions finding the same vulnerability are skyrocketing today.

**The Chair:** I'd like to follow up on that, but my colleagues also have questions and we have just a few minutes left.

Is it Mr. Spengemann, or Mr. Picard?

**Mr. Michel Picard:** Yes, I have just one quick question.

● (1700)

[*Translation*]

I will turn to Mr. Waterhouse first.

If the Canadian government wants to use the services of hackers, or security researchers, to describe them more positively, does it have to go through a process to recognize and legitimize those services? Do people have to have legitimate courses on legitimate subjects in order to have the same expertise that hackers have by definition?

**Mr. Steve Waterhouse:** If I understand your question correctly. Mr. Picard, you are asking me whether or not the government could use the services of recognized hackers.

**Mr. Michel Picard:** Right.

**Mr. Steve Waterhouse:** The contracts that Public Services and Procurement Canada enter into have to be properly done. They have to contain a section on security. A security check has to be done. If an individual, or group of individuals, works on the government's information systems, they have to have received the appropriate legal authorization to be able to do the work.

**Mr. Michel Picard:** There is another important factor.

[*English*]

I'll switch to HackerOne.

I understand that you started hacking at quite a young age. At that time it might not have been as legal as it should have been, but you managed to put together a pretty good legal company, and now you are a legitimate, well-recognized company. What kind of process did you go through to be recognized and to work with government?

**The Chair:** Are you asking for business advice?

**Mr. Michel Picard:** No, I want them to open a branch in Canada.

**Mr. Jobert Abma:** Do you want an answer from a personal perspective, or from a company perspective?

**Mr. Michel Picard:** Let's stay corporate.

**Mr. Jobert Abma:** One of the things we've been very proud of is the improvement people have seen by leveraging the hacker community to create a mature security organization, up to the point where we've seen that, even with our expertise in security, there are always problems being uncovered by other people who are much smarter or more creative than us.

The model works. Because of our relationship with the hacker community, we are able to build products that help organizations establish a relationship with the hacker community, and we essentially mediate between the two if necessary. Our success is solely through the success of the hacker community and the kinds of security vulnerabilities they have found for our customers.

**Mr. Michel Picard:** My concern is the following. From a practical standpoint, it's great. From a legal standpoint, as state with the rule of law, we have to make sure that we don't engage or contract “delinquents”, by definition, therefore legitimizing illegal activity for our own purpose and good. That doesn't work. We have to work with something legal in order to justify our actions. Did you have to go through some sort of recognition, or erasing a past file or whatever?

**Ms. Deborah Chang:** With the DOD we had to pass additional requirements. The hackers had to pass additional vetting requirements from the Department of Defense. The Canadian government can do what the U.S. government did, which is making the Hack the Pentagon series of programs very, very public. It opened up the doors for a lot of the hackers and invited them to hack on the platform. That set in motion the acceptance of inviting the talent out there that you might not know about.

There are some programs where hackers sign additional NDAs directly with the customer or client, or customers can ask only citizens of certain countries, like the U.S., in some cases. Some customers only want U.S. citizens on the platform. We work with the customer to see what makes them comfortable and then select which hackers would be best for their program.

**The Chair:** We'll let Mr. Waterhouse finish this.

**Mr. Steve Waterhouse:** Mr. Picard, we already have companies throughout the country that are engaged in white hat hacking activities. These are legitimate companies. There are no criminals involved. People are coming out from the university circuit and getting hands-on experience just as I have done throughout my life. They can provide a solid solution also, just like HackerOne.

You have GoSecure in Montreal, which is well-renowned. They are fed by people coming out of university. They are very professional, just like this lady and gentleman with HackerOne.

● (1705)

**The Chair:** I want to thank each of you on behalf of the committee, but also personally, for a fascinating hour and a half. This window into cybersecurity is getting more and more complicated the further we study it.

I'm sure that our friends in California have a much better weather window than we do.

The meeting is adjourned.

Published under the authority of the Speaker of
the House of Commons

## SPEAKER'S PERMISSION

Also available on the House of Commons website at the
following address: http://www.ourcommons.ca

Publié en conformité de l'autorité
du Président de la Chambre des communes

## PERMISSION DU PRÉSIDENT

Aussi disponible sur le site Web de la Chambre des communes
à l'adresse suivante : http://www.noscommunes.ca