National Security Cyberspace Institute
NSCI

CyberPro

November 2009

Keeping Cyberspace Professionals Informed

## SENIOR LEADER PERSPECTIVE: G. MARK HARDY

*NSCI's Lindsay Trimble recently interviewed G. Mark Hardy, president of National Security Corporation. Hardy, who holds a CISSP, CISM and CISA, has been providing information security expertise to government, military and commercial clients for more than 25 years. A long-standing industry veteran, he is a perennial speaker at major industry events and the author of* The Information Security Handbook for Enterprise Computing, Client/Server Security Handbook *and a contributing author to* Network Security Secrets. *Hardy is also a captain in the U.S. Navy and serves as president of the Association of the United States Navy. In this interview, Hardy discusses the evolution of cyber security methods, challenging security issues for organizations and gives recommendations for overcoming these obstacles. He also provides insight into cloud computing and risk assessment and gives a preview of a new information security educational curriculum currently being developed.*

***NSCI: You have been working with government, military and industry clients in information security for more than 25 years. How have cyber security methods and solutions changed in that time?***

HARDY: The methods of the attacks have changed, therefore the methods of the solutions have had to change along with them. Typically, a threat will emerge or manifest itself, causing a person to develop some sort of countermeasure or defense. At this point, those who can implement the countermeasure will do it, it rolls its way out, gets itself into the marketplace, people implement it, the threat gets mitigated and attackers come up with something else.

We have seen generations of security threats, which have gone from everything such as relatively benign, simple things. An example of this would be old, original viruses, such as the Michelangelo Virus, where the requirement was to physically transport a floppy disk from one medium to another. Someone accidentally would leave the floppy disk in one medium and infect the thing. When that happened, the infection spread by exactly 1.

As you can tell, back in those old days, things didn't change very rapidly. Today, we're in a multi-modal threat environment, where the blended threat attack vectors of perpetrators are highly complex. They rival almost a military operation in their sophistication and require a very comprehensive, blended response to be able to deal with them effectively.

Many organizations lack full-time security staff. Those who do have full-time security staff don't always have folks who have been trained at a high enough level to respond to the threat and, most of the time, those are the last people in an organization to discover that there is a problem. Typically, it's a user, somebody who has little to no security expertise – maybe a secretary or a salesman – that will encounter something that looks relatively irresistible: "Click here for free tickets; Click here and watch dancing bears."  Nine out of 10 people will click to see what happens when you click on dancing bears.

That’s when a new infection breaks out, runs through an enterprise and effective responses are required.

We’re also seeing a change in the threat environment from the 1970s, when we started doing security. To define terms carefully: “Crackers” are those who do malicious work. “Hackers” are those who can produce an outcome that the designer of a system didn’t intend.

For example, Einstein hacked Newtonian physics. Newton wasn’t thinking about what happened when things moved close to the speed of light. But Einstein was thinking about it. He said “What if I do this?” and, sure enough, he came up with a solution that essentially hacked Newtonian physics and produced an outcome that the designer didn’t intend. It produced something useful for Einstein – his theory of relativity.

So, when somebody hacks a computer system, they’re not violating laws of physics; they’re not changing the wiring on a chip. You can’t do that; you have to work within the rule set, but yet you’re still producing an outcome that the designer never thought possible, because our systems are so complicated.

In the 70s, hacking’s focus was based on intellectual curiosity/proof of concept – “Hey, I can break into this system.” The hacker ethics back then was “Cause no damage and don’t take anything.” It was a little bit like seeing if you could pick a lock; you’d get the neighbor’s door open, but then close it back up again. You just wanted to see if you could do it. You didn’t break or take anything.

In the 80s, it became a little bit more like pranks. It became more like “Look what problems we can cause.” In the 90s, it became malicious. People were hacking Web sites, defacing things, putting up obscene content. By the 2000s, we saw the emergence of almost full-scale economic warfare on the Internet, whereby organized crime were attacking using the Internet.

You know when they asked Willie Sutton, a bank robber, why he robbed banks, he said “Because that’s where the money is.” If you ask the criminals who are going after the Internet why they’re hacking, they’ll tell you “That’s where the money is.” It’s in the computer systems, so we have a different type of threat going forward. We have not yet seen this, but the manifestation for the 2010s is likely going to be cyberwar. We’ve seen the first couple rounds of that with Estonia and Georgia. Interestingly enough, the world community didn’t respond with military or economic sanctions, or even strongly worded diplomatic protests. That sends the wrong message to those who would potentially use cyberspace as a battlefield.

***NSCI: In CyberPro, we’ve had a couple interviews with leaders who agreed there will be a need to develop national and international rules in cyberwarfare.***

HARDY: It does breed some interesting legal questions because where is dot.com? Nobody can answer that because it no longer fits within the construct of our classical legal system, which defines certain activities or certain actions as taking place in certain territories and therefore describes where the domain is that the courts have jurisdiction.

For example, if you look at the situation in Georgia, where the government came under electronic attack, then is that under the United Nations or NATO? Is that Article 5 – collective self defense against an armed attack? Article 6 also talks about armed attack, but it focuses on territory. What about cyberspace? It turns out that when the Russians attacked the Georgian Web servers, a Georgian national who happened to live in Atlanta, Georgia – how about that? – reposted all of the Georgian Web sites. If that were under legal terms of armed conflict, did that person just engage in an act of war by aiding one side of an armed cyber conflict? The answer is: We don't know.

It's an emerging field that has to be defined. As you know, the U.S. has recently stood up the Defense Department's U.S. Cyber Command. The U.S. Cyber Command will be a sub-unified command, which means little to anybody except if you're in the military. Fundamentally, it means that all Services will be represented, it will be run by a 4-star and it will have central authority to protect military critical infrastructures. The problem is complicated because probably 90 percent of our country's critical infrastructure is privately owned. Who owns the power grids? Who owns the electrical system or the stock market trading networks? Those aren't necessarily owned by the government, so how do you work out agreements to protect that when they're a potential target for a cyber attack?

***NSCI: What are the top two or three actions you think the Obama administration should take to improve cyber security?***

HARDY: The first thing is something they've already done. The administration has identified cyber security as a national issue.

With that identification of the problem comes the second step: the ability to develop solutions. The direction of the Secretary of Defense to stand up U.S. Cyber Command is a big step in that direction in the military.

For the civilian world, we're still looking for an effective cyber security – I'd like to use the word "czar," but the problem with that is creating a position with responsibility and accountability, but with little or no authority. It's a difficult issue. As we discussed previously, 90 percent of our critical infrastructure is privately owned. How do you end up with a cyber security director who has authority to make decisions that are going to affect those private companies? You can't order them to disconnect this, or to use that, so bringing together some of the best experts to work out these issues in advance is important: How would we deal with this type of attack? How would we deal with this type of infrastructure issue? From that, we develop and take decisive courses of action to build into our national infrastructure the ability to withstand and sustain a potential attack and to build alternative resources for our country, so that in the event that we face this situation in the future, we don't have to go the way of Estonia and Georgia and just have to wait for it to end.

***NSCI: I think we're all waiting with bated breath for an official announcement about this position.***

HARDY: Everyone's waiting to see, but the problem is we talk about the CSO as the "chief security officer," but I think for many organizations, the CSO is the "chief scapegoat officer." It's the person you blame or the person you fire when something goes wrong, and yet that person didn't have the authority to correct the issue in the first place; they were in an advisory role.

That, again, comes back to the scope of authority. A security leader with appropriate authority will work. Let's look at Cisco Systems as an example. Their corporate vice president for security has the authority to shut down the entire Internet access to the company. He had to do it one time, when the SQL slammer worm infected computers all around the world in minutes. Cisco does a large majority of their business online. This outbreak took place during their busiest sale season and he had to make the decision to cut off access and, therefore, cut off all orders coming in, which would cut off revenue, which would cut off bonuses. It was a very unpopular action, but it turned out it was absolutely the right thing to do. The chairman of the board supported the call and that's an example of how to do it right. You have a head of security that has the authority to pull the plug and acts with the authority of the chairman of the board or acts with the authority of the president.

***NSCI: As you routinely speak to a variety of audiences, what are the most challenging issues they ask about? What advice do you have on steps to take to overcome these obstacles?***

HARDY: Audiences are concerned with the fact that they often lack the resources, financially, to fully address their problems. That lack of financial resources is traceable to poor communications with executive management, in that few people can articulately translate a technical aspect of a security issue in actionable business criteria.

So, if someone were to bump into the president of the company in the elevator and say "We just had a tweet on Twitter that came over this particular blog that has some posting off of someone else's site that suggests there's some information out there that shouldn't be out there," the president would probably have that "crazy" person escorted out of the building. By effectively rephrasing, you could say "We have an intentional e-mail liability that could potentially disclose information that would cause a shareholder lawsuit, disruption to our revenue and decrease our stock price." Now you have that executive's attention and have explained the exact same event. You've just rephrased it in a criterion that is actionable.

Much of what I personally do is serve as that "Rosetta Stone." I have a business background, an MBA, have worked with a variety of organizations and am also certified as a security expert (CISSP, CISM, CISA). I can speak credibly to both audiences and also transmit information from one side to the other; it's not as easy as it seems. As a result, one of the big issues for many individuals, and therefore organizations, is that they cannot bring to bear the necessary resources to protect themselves.

Second, it comes down to education. We're seeing a concern with respect to how do we find smart, educated people to do cyber security work? The federal government recently said we need 1,000 smart new people. There's some discussion saying they're not out there. They are, but they're already employed and are probably already making good money. Or, they're hackers and they're probably not going to be able to pass security clearances. Again – not using hackers in a pejorative term – but in general, these may be folks who developed security expertise in an "extracurricular" fashion, people whose personal backgrounds may not qualify them for a security clearance, or people whose social skills are less than desirable in corporate America. They may be brilliant online, but face-to-face may not be highly successful as a communicator.

So, part of the issue is developing education and creating pathways for people in the workforce and for new people entering the workforce. We're seeing an emergence of educational opportunities designed to create a cybersecurity workforce, but that takes time. There is a vulnerability window, whereby our ability to respond may be inadequate to the potential unknown threat that's out there. We can get there from here, but we'd better get working on it now!

***NSCI: What advice would you give to overcome that education and training obstacle?***

HARDY: I'm taking action on that. I am working on a project that is building an entire cyber security educational program at the bachelor's degree level. We're creating 13 courses, with 13 subject matter experts and a publisher. Major colleges and universities nationwide are going to be able to distribute this. We're also creating online hands-on laboratories that allow people to learn kinesthetically how to do it, instead of just reading it in a book. And we expect to have this up online by next fall. It's a very ambitious project, but rather than simply wringing my hands and saying "Woe is us," I'm moving forward and taking action. We're still working out the details, but the major pieces are in place. This will create a significant opportunity for people entering the workforce as well as, ideally from my perspective, military veterans who wish to transition to the civilian workforce or who wish to return to the military in the cyber workforce. We'll provide access to educational programs that, currently, are very difficult to find in the educational market today.

***NSCI: Looking at the future of IT security, how do you think our universities and various certifications (e.g. CISSP, CEH, CISM, CISA) are doing in preparing future cyber security professionals?***

HARDY: Initially, I'll ask the question "what does it take to create a certification?" The answer is critical mass.

The CISSP – when it was first developed 20 years ago – had a very slow start. It took about seven or eight years before it caught on. The SSCP certification – which is also administered by $(ISC)^2$ – has had a slow start, but we expect that to start catching on.

Certifications provide assurance to a potential employer that an employee had demonstrated a certain level of knowledge and maintains currency in that knowledge. How do we translate security certifications into preparing security professionals?

The Department of Defense has issued a directive – DoD 8570.-M. Basically, 8570 specifies industry security qualifications because the Department of Defense doesn't have, within itself, the ability to issue certifications. However, they recognize a certain level of due diligence in the commercial marketplace that certain certifications represent a level of demonstrated expertise. Many of these certifications are brought to bear in the Defense Department by meeting certain criteria. We have three levels of workforce certification for the workforce and for management. We have that particular instruction broken up into different categories: IAT for technical; IAM for management; with increasing certification baselines for Level I, Level II and Level III.

All of these are very useful for a senior manager, in that when they look at the alphabet soup of certifications out there, it translates those into a roughly parallel expertise. For example, CISSP would be an excellent certification for a high-level manager in information assurance, but is probably not the right certification for an entry-level technician. And so having something such as DOD-approved baseline certifications helps management – whether they're in the government or the civilian world – sort out the alphabet soup of certifications to match them to the level of expertise they need.

***NSCI: Should there be certifications for certain security professionals, such as those working critical infrastructure?***

HARDY: If you look at what makes a certification work, it has to do with critical mass. There is now a Certified FISMA Compliance Practitioner – CFCP – and one can be grandfathered under the CFCP by December 31. Right now, it's an "exam" that tests for competencies of understanding certification and accreditation concepts related to the Federal Information Security Management Act. The federal government may say "so what?," but there is an organization that has set this certification up. And you can look at it and ask "Is it for a for-profit or for a non-profit organization?" The answer is it doesn't matter. (ISC)$^2$ is a non-profit, but there's no reason you can't set up a vendor certification declaring it's a standard and make some money off it.

So you find that certifications do a couple of things. First, they may serve industry by assuring a certain level of knowledge. Secondly, they also represent a pretty decent revenue stream for an organization that gets everyone to buy into it. And so, if we assign a certification to certain job skills, there may be value in that, in that it demonstrates a deeper level of understanding. But it further clouds and complicates the marketplace and there is no central unification for all of these skill certifications.

For example, think of someone going to the drivers' license bureau and saying they want a drivers' license to drive a bus, a dump truck and a motorcycle. For the most part, if you want to drive a bus, a truck and a motorcycle – in whatever state you live in – you're going to have to prove the same level of expertise. You really don't have a chance to come up with shortcuts.
So, who's administering these certifications? How do we know the material is current and up-to-date? And where does the money go? Certifications help, but I suggest that's not it. There are many courses now where one can take a boot camp – four-day, intensive training, on the fifth day, they whisk the materials out from under your face and slide the test to you, you regurgitate it as fast as you can with

your short-term memory, you pass the test, and congratulations! But is that true learning? I don't think so.

The difficulty we face with certifications is that it means that if a person passed a particular test at a particular time, it doesn't necessarily demonstrate ongoing competency. That ongoing competency is normally assured through continuing education – accruing 40 credit hours per year, for example – by attending conferences, writing things, reading things, learning things, attending classes, etc. There's a whole range of doing that, but it basically shows that an individual has demonstrated dedication to learning.

These qualifications are, for the most part, self-reported and enforced through random audits. It's possible that someone could have a certification, be brilliant, work on this 52 weeks a year and has been doing it for 20 years, and their exact same certification could be held by someone who took a four-day cram course, regurgitated it on paper and kind of stretched the truth from time to time to show they stayed current, but nobody really knows. The real difficulty for the employer is a certification should assert a certain level of expertise, but with the caveat "let the buyer beware." Have that person demonstrate, ideally hands-on, how they would handle types of issues and problems that one expects. Successful passing of that real-world test is probably even more important.

***NSCI: What advice would you give to someone interested in pursuing a cyber career?***

HARDY: Good question. First, commit yourself to lifelong learning. Moore's Law states that the density of transistors doubles every 18 months, and therefore computing speed doubles in the same period. G. Mark's corollary says half of what you know about information security will be obsolete in 18 months. For those who don't believe me: two years ago, how many Vista computers were being run? And now, how many Windows 7 computers are being run? And, yet, roll the clock forward 18 to 24 months, and all the numbers change. iPhones are barely two years old, and  yet they're ubiquitous. Twitter was unknown two years ago. What comes after Facebook, Myspace and Twitter hasn't been invented yet, but two years from now it will have 20 million subscribers. So, that first commitment has to be to constantly learn. One can't expect to say "I have an education; I can do the same thing over and over again."

Number 2: have an ethical orientation. People want to be hackers, do penetration testing or break into things because it sounds like it's fun. And it is. But, outside of the proper context, it's also illegal. I advise people not to stray to the dark side early on in their lives. An arrest record or errors in judgment may prevent them from ever having an opportunity later in life to do work that really means something – for example, earning a Department of Defense security clearance and working with some of the most sophisticated security systems ever invented.

The third piece of advice I would give is get an education. Many people who get into security have a tremendous knack to learn computers at a young age, but they may not have the personal discipline to sit through social studies, algebra, etc., and don't succeed academically. The older I get, the more I realize that having a well-rounded education offers the most opportunity. For those who do not have a degree, go get one. Security degrees are going to become much more available in about 10 months when we roll out comprehensive security education – a capability that will reach several hundred cities across the United States. Having an education and the discipline one learns when going through that education is going to help maintain that lifelong learning aspect toward doing things. That, plus an ethical background, pretty much positions a person – if they're competent – to have a very successful career in a variety of agencies.

***NSCI: In your risk assessment work, can you tell us about a few of the best practices you've seen that all organizations could or should be implementing?***

HARDY: Number 1: Have a written policy. A written policy defines what's important, what needs to be protected and how important it is, therefore how much value is assigned and how much to spend to protect it. Effective policies should be about one page long. People say "How can a policy be just one page?" And I ask "What is the attention span of the average executive in pages? The answer is one."

And so, what that suggests is that having a brief policy statement creates the expectation that all employees should read it. Policies should be simple; the details can be worked out. Policy statements answer a number of basic questions. They have to match the mission of the organization. Policies should be written with a good understanding of the business, rather than simply written by security people. That's why we end up with policies that say "15-character passwords, 3 uppercase, 3 lowercase, 3 numbers, 3 special characters, and must be changed every 30 days." Well why? It's good security, but people don't think that way. We have to get details from reality. Write that policy in a way that defines what you protect, how much it's worth and make sure every employee reads it and knows it. That's probably the most important thing.

Secondly, focus on security awareness and training. Most people want to do the right thing, but they are very bad guessers when it comes to knowing what the right thing is with respect to computer security. So, given the choice between deleting without reading or clicking on dancing bears, I think that some employees tend to click on dancing bears to see what happens. Unfortunately, usually something else happens other than just the bears dancing. The education needs to be recurring, and ideally, security awareness becomes a part of the corporate culture. Certain companies and military organizations have their own culture.

When I fly with Southwest Airlines, for example, their culture is to take care of their employees and they'll take care of the customers, and have fun doing it. And it's a fun airline! They sing the departure song, they tell jokes, they'll toss peanuts down the aisle, and everyone expects that. But if you fly on another airline, they're absolutely business-like. That's their culture. Defining the culture needs to have security awareness as part of it.
The military is very good at that. When I was on a ship years ago, you'd answer the phone by saying "This is the quarter-deck. This is not a secure line. May I help you?" What does "This is not a secure line" mean? When you answered the phone, you told the person on the other end that somebody else might be listening in; everyone on the phone call knew that they were potentially subject to monitoring. Now, we send e-mails with large important attachments and who knows who gets to see it along the way? Awareness and training will help.

And then the layered security tools come into place. What the security technology will do is keep the honest users from making serious mistakes and make the dishonest user's level of difficulty higher when they're trying to commit a hostile act. There's no getting around it, but you will keep the honest people honest. For example, locks keep honest people honest, but they don't keep all the thieves out. The goal of layered security is to create a gauntlet of multiple security challenges an attacker may fail to complete because they lack the time or the skill to complete it, or they set off an alarm and provide for a response, so they can't get to their objective.

In summary: have a written policy; training and awareness; and layered security.

***NSCI: How does risk assessment scale from a small business network, with a couple of a servers and a few dozen clients, to something as large as the DoD, operating across multiple networks with hundreds of thousands of clients around the globe?***

HARDY: Risk assessment is fundamentally matching vulnerabilities to threats and to assets. How much is my asset worth? What are the threats that could cause harm to that asset? And how vulnerable am I to those threats, that is to say, can they manifest themselves?

For example, if I lived in San Francisco and had a collection of fine crystal, the threat to that may be earthquakes. Well, there's also a threat of earthquakes on the east coast, but the vulnerability – how likely is that to happen to you – is much higher in San Francisco than it would be in Washington, D.C. It's still there, but a risk assessment looks at it and helps you decide whether to prepare for it or not. If it happens, then you take the hit. It's a management decision whether or not to accept the risk. If one decides the risk is unacceptable, then risk assessment says you need to mitigate the risk – implement a countermeasure; assign the risk – take out an insurance policy; or avoid the behavior. And that is the only way to really do risk avoidance.
If you're afraid of dying in a plane crash, never fly on an airplane – that's avoidance. But if you never fly on an airplane, you might have a hard time living parts of your life. But that's a choice you can make.

What we do when we look at something from a risk assessment perspective is know what your assets are in terms of their value; know what the threats are; know what the attack vectors are (i.e., what's your vulnerability to them?); and understand the universe of countermeasures available. Then you can make a series of business decisions on what countermeasures are reasonable to implement and provide a reduction of the risk; what risk are we going to assign to others; and what risk is of such a nature that I can neither reduce it nor reassign it, and therefore must stop that particular practice – that's risk avoidance.

***NSCI: You've authored books on various aspects of information security. Given cloud computing seems to be catching on, what are the major security changes an organization should be aware of prior to adopting a "cloud architecture"?***

HARDY: Many people don’t understand what cloud computing really is. That may be the biggest danger. Basically, what happens is that in the traditional technology infrastructure, one owns a computer, they own the software applications, they plug it into the wall, they have to do the maintaining and updating; all this work you do yourself.

Cloud computing says you don’t need to understand that and you don’t have to have the technology. Someone else will provide it for you. It’s out there in the “cloud.” But what is the cloud? The cloud would be someone else’s computer system that is providing you the service. It’s transparent to the user where that service is coming from or even the computer it’s running on. For example, software as a service would be something like a Google app. I don’t need to own Microsoft Word. I can just log into Google and start doing word processing. It’s stored on the Google server “out there in the cloud somewhere.”

In a nutshell, that’s pretty much what Web hosting has been for years. Very few people have their own Web site hosted on their own computers; it’s done by somebody else. Now we’ve extended that to a whole range of computing capabilities where the end user or the head of a business doesn’t need to know where it’s being run, where the system is or who’s running it. They just know that when they plug it in, it’s turned on. It’s like electricity: when you turn on a switch, you know it’s there.

What about security models for cloud computing? The problem is that we don’t have any yet. We’re working on it, but what happens is that with a third party hosting your data someplace else and probably co-locating your data with many other customers, how do you keep somebody – such as a skilled hacker – from entering your database, climbing outside of that enclave and then climbing into someone else’s database.

A lot of cloud computing is moving toward virtual systems, using VMware and other types of tools. If you wanted to have a new Microsoft Windows 2007 server with 2G of memory and 50G of hard drive space, and an Oracle database solution up and running, it’d take you about a week. You’d have to call Microsoft and Oracle, have it shipped, installed, configured, and update the software. In the virtual domain in cloud computing, you’d go online, say “give me this…” and within minutes, you’d have a virtual machine, out there in the cloud, ready to run.

Security will be tough. To whom do you assign liability? What are the international boundaries? If the attacker is from overseas, how do you catch him and in whose court do you prosecute? How do you enforce a service-level agreement? There are a number of potential security issues starting to emerge as we look at it. You can encrypt data at rest, but you can’t work on encrypted data, so if you’re using software as a service, someone has to decrypt the data before they can process it. While it’s decrypted, it’s potentially vulnerable. What about personally identifiable information? Or other databases that fall under regulations, such as HIPAA, or financial information subject to the Gramm-Leach Bliley Act

(GLBA)? Some of these companies might be compromising sensitive data or getting it wrong, resulting in criminal charges. If the lack of data integrity is due to a hack at the cloud, to whom do you assign liability? The point is it's a great paradigm, but we're still figuring it out. I would love to see a conference focused on cloud computing security.

***NSCI: Is there anything else you'd like to add?***

HARDY: Security has evolved over many years to go from the fringes of computing to being part of the core of how we have to do business. The Internet has been urbanized. We've gone from small-town America, where you can leave your front door unlocked and the keys in your car overnight and never worry. Today, we lock our car, take the keys, set the alarm in the house, put bars on the window, and you still have to worry about attacks. With that as a paradigm, security becomes much more important. Not only that, but we put much more of our lives, information, business process know-how and critical infrastructure of our national defense on the wire. I fully expect the next war to be on the wire. Having access to qualified cyber security experts will be critical to protecting the critical infrastructure and the industrial knowledge-base of America.

The average person doesn't yet see cyber security to be anything more than perhaps a compromised credit card number, or at worst case, identity theft. It has the potential to drastically impact lives, where it takes out huge chunks of critical infrastructure. We must – as a nation – prepare for that, defend against that and enable our workforce to be able to succeed, fully-functioning, in a hostile environment before that environment materializes. The danger of it is that people wait until some adverse event happens before they protect against it because denial often exceeds wisdom.

I hope we don't have to go down the road of a digital Pearl Harbor before it happens. It's unfortunately likely that it does have to happen. We've seen the first couple of shots fired – Estonia and Georgia – and the average person is not yet alarmed. I'm working with a team to build a pathway to educate thousands of cyber security experts, allowing them to get bachelor's degrees in information security. I'd love to chat with you in the future and give you more details, as we've got something big on the horizon.

Thank you.