@Risk: Risk Networked with Shuman Ghosemajumder

[Music]

Jodi: Hey, I'm Jodi Butts. Welcome to @Risk, brought to you by Interac.

The scale of cyber risk events are as limitless as the networks to which we personally belong and on which our civic institutions and economies rely. Cybersecurity breaches may quickly beget financial risk at personal as well as societal levels, and even lead to larger geopolitical risks. Given that risk is distributed as quickly as fortunes are made by network effects, is it time to adopt new approaches to how we protect and sustain cyber security? Can we leave something as important as cyber security to the same sector that valorizes moving quickly and breaking things? Is it time to move beyond talking about cyber security as a matter of personal or even individual corporate responsibility?

To explore these questions, I'm joined by Shuman Ghosemajumder. Shuman is the global head of artificial intelligence at F5 Networks. Previously he was an early product manager at Google, helping to launch Gmail and leading global product management for click fraud protection. He is a regular guest lecturer at Stanford University, and in 2011 the Boston Globe named him to their MIT 150 list as one of the top innovators of all time from the Massachusetts Institute of Technology.

Shuman is optimistic cyber security can keep a pace with the evolving threats to it, but he has some cautions to share with us. We should listen.

Well, thank you for joining me Shuman, and welcome to @Risk.

Shuman: Thanks for having me.

Jodi: So let's just get right into it. How worried are you about the coming shifts in the risk cyber security equation, particularly as we think about maybe some of the new technologies that might be coming online?

Shuman: I wouldn't say that I'm worried. I think that I'm very mindful of how new technology creates new opportunities for cybercrime and creates new risks that we have to be mindful of. But I think that the level of awareness of cyber security in general is at a higher point than it's ever been and only increasing.

I think that whenever we're discussing the impact of new technologies, there are various categories of impact that we have to think about. We have to think about the impact on society, we have to think about the impact on the economy, and of course now we think about sort of secondary effects in terms of what are the cybersecurity risks, and what we call the attack surfaces that are introduced by new technologies.

But I think that we're having those conversations earlier and earlier now, and having those conversations on a societal level. So I think it's actually a very positive sign. And I think that we're going to be able to create mechanisms that allow us to be able to get the benefits of new technologies without having to be overly worried about how cyber security could become a crippling issue. I think that we have good ways of allowing both cyber security and technology to continue to evolve together.

Jodi: Now, you mentioned a widening attack surface. Can you please explain what you mean by that?

Shuman: Sure, so in a cyber security context, whenever there is a new opportunity to be able to create some type of hack or to be able to identify a new type of vulnerability that can be exploited, that's what we refer to as an attack surface.

So if a company launches a new website, that's a new attack surface. That's a new way into their data store, that's a new way into their user information. And if you want to remove that attack surface entirely, the only way to do that is to shut down that particular website or application. And so instead of doing that, because, of course, shutting down that attack surface would have implications in terms of that company's ability to do business, what you want to do is secure that attack surface.

Now of course, you don't want to have redundant attack surfaces or have duplication in terms of if you can do something with one particular website, you don't want to have 10 different websites that do exactly the same thing. Because then any security vulnerability that exists in any of those attack surfaces creates the opportunity to be attacked that you don't need to have. So you might consolidate multiple websites that do the same thing into a single website, thereby reducing your attack surface, and then try and protect that attack surface as effectively as you can.

Jodi: Just reading in magazines and newspapers, folks are talking about the internet of things, and your refrigerator is keeping track of things, and your TV is as smart as it's ever been. Are these all attack surfaces?

Shuman: They can be, it all depends on what those particular applications have the rights to be able to do. So for example, if you've got a smart refrigerator and that smart refrigerator is keeping a list of all of your groceries on a regular basis and it's storing that in a set of servers that are hosted in some cloud service, then if that smart refrigerator gets compromised, the attacker is now going to have access to your list of groceries.

So you might not think of that as a particularly big deal, unless you've got some embarrassing groceries or something, I can’t imagine exactly what that might look like. But there are secondary effects from that that you might not think of right away. So let's say that the password that you use for your smart fridge account online is the same password that you use for your bank account. Now all of a sudden that attack

surface being compromised not only creates the opportunity for someone to publish your embarrassing grocery list, it might give them the opportunity to take over your bank account and steal all your money. And so of course that's a lot more serious.

And this is one of the things that we've seen over the course of the last 10 years is that what you might not think of as a serious attack surface can actually be a lot more serious than you realize. And so the interconnectedness between different applications and different companies, that creates new levels of risk when it comes to those attack surfaces.

Jodi: Now just even in that example, you highlight how what is a cyber threat can be a privacy threat, as we joked, if you're concerned about your grocery list. But it can also then become a financial risk. And I noticed in the paper that you contributed to with the World Economic Forum, that they really looked at cyber security and its related risks as a challenge to financial growth.

Shuman: Absolutely. I think that you have to have certain levels of cyber security in place in order to be able to engage in certain types of commerce. So you look at the way that banks approach cyber security, for example. And a large-scale hack of a bank is a of course an existential risk for the bank, but it's actually an existential risk for our entire economy.

So you think about the way that banks are perceived, and how big a hack would you have to have at a bank for people to start to lose confidence in the idea of banking and to facilitate a run on the banks, and something with disastrous impact for the economy as a whole.

And of course, that's something with the way that information spreads so quickly now, and misinformation as well by the way, that could result in a worldwide ripple effect.

Jodi: So one of the questions that I was left with reading that paper is are we just getting a little too ahead of our skis? So that paper talks about things like always-on connectivity, quantum computing, and looks at cyber risk through the lens of these new technologies that are not off in the far distant future, but we're on the cusp of. And it just made me ask myself, like there's the ability to do things, but can we do them securely?

Shuman: It's a great question. And I think that we can do new things quickly and securely, but we need to approach it in a different way than we have traditionally. I think that we're still stuck in the mode of every company thinking that the way to be as secure as possible is to try and hire the most talented cyber security team that they can and scale that team with as many resources as they can provide them.

But let's say that you do that across the Fortune 1000. What that's going to mean, by definition, is that one of those companies in the Fortune 1000 is going to have the 1000th worst security in terms of the level of capability that their team has. And that's

simply not acceptable for large companies, especially companies that are so interconnected now.

And this is one of the things that we've seen with hacks like the SolarWinds hack. If you've got any sort of technology in your infrastructure, and everyone's infrastructure now consists of hundreds of different technologies that enable modern corporations. And if that technology has a level of access that allows it, if compromised, to be able to create very profound and disastrous effects, then it's simply not acceptable to leave the security of that particular technology to that organization's arbitrary level of resourcing and capability.

We need to have a more platform and services oriented approach where you can have the very best security that is available provided to everyone in the technology industry, everyone who is using products from the technology industry. And that's the way that you create much more of the network effect associated with the knowledge around cyber security.

So think of the way that we approach securing buildings today. We don't go to banks and go to any large company that needs to be able to create physical security in their building and say that you are now responsible for manufacturing your own locks that are going to be placed on doors. There are industry standard ways of creating locks, and actually different levels of security that are associated with different types of physical locks. And there are specialist organizations that manufacture those locks and everyone uses them. It should be the same thing for multiple levels of cyber security practices and ways that we secure technologies.

And I think that as a society and as an industry, we're just figuring out how to be able to create those processes and services so that everyone can benefit from them.

Jodi: And is there a role for government in this, or does it really need to be industry-led when we think about setting those standards?

Shuman: I think that there is a role for government, but it may not be the role that government has traditionally had when it comes to other types of problems and other industries. One of the main challenges is that technology in general moves much faster than the law. It moves much faster than legislation, and certainly elected officials are not going to be experts in technology.

There's no way, regardless of how many hearings you have, to be able to make them experts in technology. Especially considering that a lot of the decisions that you have to make that are going to govern the way that the technology industry functions have to be made not only with an understanding of what has happened in the past and negative effects that have occurred, but also with some kind of vision for what could happen in the future.

So I think that the role of government can come in the form of expressing society's expectations, expressing at a general level what is acceptable on the legal front in terms of industry behavior, but then it's going to be up to the industries themselves to figure out how to operationalize that in the context of specific technology solutions.

So when it comes to cyber security, I think there are various categories of standards that the industry could work on in collaboration, with government to some extent, but then primarily working within the industry and across specialist companies to figure out how to be able to create the best versions of those technologies at every given point in time so that every other company can benefit from them.

Jodi: Is there enough incentive to really invest in security? It's just one question that always nags at me. Because there's certainly, I mean I think this is true across all sectors but certainly in the technological sector, the focus on speed. And the focus on data, like so many revenue models rest on collecting as much data as possible. Doesn't security sometimes become more of an afterthought or viewed as an obstacle?

Shuman: So it traditionally has been. It is essentially a trope in the security industry that security teams aren't hired, or even when they are hired, they're not brought in until very late in the product decision-making cycle. And that's something that large companies are certainly changing or trying to change. But the industry as a whole still has this challenge.

I think that when you consider a new product that you want to create or consider the way that a start-up typically brings an innovation to market, they don't start with a security team. They don't have the resources to be able to do that. If you've only got a handful of engineers that want to demonstrate that you can do something new and innovative that's never been done before, you don't start with any type of compliance process or any type of supporting process. You don't go and hire a legal team, and you don't hire a finance team. You try and hire the very best engineers that you can and develop the capability that shows what makes it unique.

And only after that capability demonstrates that it adds value to the world in some way that people are willing to either adopt or pay money for, only then do you add those supporting functions. And security has traditionally been one of those supporting functions. In fact it's often been a supporting function that falls way down the list after taking care of legal concerns, taking care of financial concerns, marketing concerns, and so on.

And I think that the way that you address that is by making it a lot easier for security to be built in. You get security more automatically from your platforms, and you get them from the way that start-ups are able to bring new innovations to market automatically.

An example of this is you look at the rise of public cloud platforms like Amazon Web Services and Google Cloud Platform and so on. And they are now providing a bunch of bundled capabilities and services that allow start-ups to be able to create applications more quickly than has ever been possible in the past. And in the process of doing that, they also provide security that a start-up would otherwise have to build into their products manually themselves. And so I think being able to get more and more of those capabilities from your platform, that's one of the keys to being able to get something that's more secure from the very beginning.

And so you look at the example again of physical security. And when you're in a work sharing space, the physical security is provided by the company that's providing that service. And then you end up with a much higher level of physical security than any small company that was trying to find its own office space would ever choose to invest in at that stage.

Jodi: Now you mentioned the SolarWinds hack, and I have to say other than obviously healthcare workers, I think security folks might have been a close second in terms of the holidays and being busy during that that period. And what happened?

Shuman: So SolarWinds was a great example of one of those very commonly used technologies that had a level of access that allowed an attacker to be able to do something very profound and disastrous which was execute code inside of sensitive environments in federal agencies and companies across the industry.

And the software itself you might think of as relatively benign. It's IT infrastructure monitoring software. But the way that it works is there's an agent, which is basically a program that's installed in each of the different companies environments that are being monitored, and it communicates with the SolarWinds system that allows it to be able to push out updates as well as being able to get information back from each of those environments.

Now what happened was there was an update that was sent out to that program that contained malware. And that malware allowed the attackers to be able to execute code inside of each of those environments. And until that hack happened, most companies weren't even thinking about the use of SolarWinds or similar technologies within their stacks in many cases. And so now this represents a new type of compromise for many companies that they didn't think about before. But it's actually a similar pattern, as we've seen, with many hacks in the past where there's some supplier that is providing you with services who has a level of access that a third-party attacker is then able to exploit.

And so I think that in this particular case, what was surprising to a lot of folks was just that SolarWinds was a company that they hadn't heard of before. But it was actually present in more than 300,000 different companies. And this particular software that was compromised was present in more than 30,000 companies. And it seems like as a

result of that more than 18,000 companies actually received the compromised binary of that software. And so that creates a level of risk and a level of compromise that is at the very high end of compromises that we've ever seen across the industry.

Jodi: It's almost like a tale of two cities. I've read on the one hand that this hack, just as you described, but that it's been identified now. People are pulling the malware out of their system, and integrity will be re-established. But I've also read some folks who I guess hypothesize that in addition to the espionage, the peeping that was occurring, it's also possible that new back doors were also created. How do we make sense of that? How do we know in what situation we're in?

Shuman: It's really difficult to know exactly which situation we're in. It's absolutely possible that additional back doors were installed, and given the level of sophistication of the attack I would say it's even probable that there are additional back doors that were installed at least in some environments that we haven't discovered yet.

So basically, all we can act on is what we're able to observe. And if you've got an adversary who's sufficiently sophisticated, they're going to know that we're looking for things to observe, and they're going to cover their tracks when they install those types of back doors.

So you look at the malware that was distributed through the compromised SolarWinds software, and one of the things that it did was look for antivirus software and other types of software that are specifically looking to detect malware. And in those cases, it would hide itself more effectively.

So this is something that is definitely a cat and mouse game, but it's a very sophisticated one. And I think that over time we're going to learn more and more about these back doors that haven't been discovered yet.

And the only way to have absolute security, like I said, is to shut off a particular system. And that's obviously not possible on a widespread basis. So we have to figure out what is possible as an intermediate step. In many cases, it is going to involve wiping servers and reinstalling applications from scratch. That's one way that the industry in general is able to get to a higher level of confidence that a given machine is no longer compromised.

Jodi: And so the hackers, it's been alleged that they're Russian hackers. This would seem to be a good example of where cyber risk potentially turns into a geopolitical risk.

Shuman: Yeah, and one of the questions that always comes up whenever you've got a large-scale hack that appears to be caused by a nation state is how do you respond as a country? And what we've seen here is the exact same pattern as we've seen in all other hacks, frankly, that are associated with nation states. Which is that the nation states who are accused of perpetrating the hack simply deny it, and then there's not much recourse you can take because it's difficult to have hard forensic evidence that a

particular entity or individual or organization is behind an attack versus it's simply appearing as though that entity is behind the attack.

Because of course, when we're talking about digital information and any type of compromise where information is being overwritten, it's also possible for another entity to make it appear as though a third party entity is responsible for that hack.

So in some cases what cyber criminals will do or what nation state actors will do is they'll leave breadcrumbs that are in a different language or associated with machines in a different country that will make it look like it's someone else who's actually behind that hack.

And when you look at the level of sophistication that's involved here, certainly it's within the capabilities of any of these nation states that we've talked about to be able to create that type of misdirection.

Jodi: And I suppose this also leads to the question of when is the line crossed between espionage and conflict, you know, we use the language of attack. Is this an attack?

Shuman: Well, it's definitely an attack in terms of the action required to compromise systems on a very widespread basis and infiltrate the business processes of companies that are important to the economy, and federal agencies that are important to the national security of the country.

But then the question is what information was stolen and what's being done with that information and with that access? So there are different levels of that attack. And I think you raise a really great point that when we're talking about information being stolen, that's typically been classified in the realm of espionage. But when we're talking about actions being taken, that's something that more frequently corresponds to what's thought of as an attack. And so I think that we're gonna see over time what actions have been taken with that information and access.

Jodi: Welcome to your presidency, Mr. Biden.

Shuman: Exactly. And I think that every new administration is having to get more sophisticated about technology. And we live in a technology driven society, and that's one of the reasons that new types of jobs are gaining prominence and new subjects are being taught in schools. So when I was studying computer science and when I was studying management many years ago, there weren't a lot of courses that dealt with security in either of those contexts. And now cyber security is required in computer science programs across the world and it's offered in business schools, in law schools, even in medical schools and so on.

And so I think that the way that technology affects our lives, it's something that we're still learning about. And technology has advanced so much in just the last 30 years,

particularly with the rise of the commercial internet. I think that we're still catching up, especially from a governmental and legal standpoint.

Jodi: Yes, I think in particular, not to pick on the United States, but lots of people point to the senate hearings with Facebook and Google and look at the questions that were being posed and the sort of lack of sophistication behind them. And I guess groan, maybe even cringe a little. Right?

Shuman: Absolutely. There was a disconnect there obviously in terms of the level of sophistication of the technology companies that participate in such hearings and the understanding of technology from elected officials. And that's not anybody's fault, that's simply the way that the technology industry has evolved versus how government has functioned up to this point. And I think that everyone being able to observe that disconnect has created a learning experience.

I think that folks in government are recognizing that it's important to have a lot more sophistication when it comes to technology, but also to figure out how to be able to manage the technology and the technology industry in a way that is able to keep pace with its level of innovation.

And I think that the technology industry is fundamentally different than other industries that have had a great deal of regulation in the past that I would argue have been relatively successful in those efforts.

So for example, you look at the way that the medical industry functions. And we've been able to observe this in the context of COVID-19 in the past year. There are safeguards that are in place that ensure that the public is going to be protected against any type of misbehavior in the industry. Of course, it's still possible in limited ways, but for the most part there's a great deal of testing and many gates that need to be passed in order for a new drug to be brought to market or for new procedures to be adopted on a widespread basis throughout a country or throughout multiple countries.

And when you have those types of restrictions in place, it actually puts a limit on innovation. And that's a limit that we're willing to live with when it comes to the medical industry. So we don't want people innovating too quickly, really, when it comes to creating new drugs and creating new surgical techniques. We don't want people creating new surgical techniques in their garages. We want to make sure that this is all done very carefully. And that not only allows us to be able to protect the public, but it allows the public to have confidence in the medical industry.

Now when it comes to the technology industry, we have different standards when it comes to people wanting to get the benefit of new technologies and the ability for a given country's technology industry to be competitive with technology industries around the world.

And so I think that we're trying to figure out how can we keep that same pace of innovation going while also inserting new processes and technologies that safeguard security. And one of the ways that companies are doing this is by understanding how they can build on top of the work of other companies more and more.

Open source is a great example of this. So you look at what many companies have been doing over the course of the last 10 and 20 years, and they haven't functioned the way that technology companies used to function where they have to build everything themselves. Instead what they do is they can take a set of open source technologies that they can freely use, and then use platforms like Amazon Web Services and Google Cloud Platform, and they can very rapidly create something where they add their own unique value from a technology standpoint. But the overall technology solution is not only much more sophisticated than they would ever be able to create on their own, it's also more secure and more capable because of all of the work that others have performed in building that complex technology stack.

And so I think that we'll see an extension of that approach as government gets more involved. And I think that there's an opportunity to be able to set some standards that say that here's what companies need to do, or even what we recommend companies do. Government recommendations can be very powerful as well in terms of guiding what society's expectations are for a given industry. And that can get down to the level of what we want from a security and privacy perspective.

Jodi: The health example is a very interesting one because even before you kind of get to that FDA or Health Canada approval stage, you've moved through a research process, right? So if your research involves human subjects, it's a very rigorous process. But even if your research only involves the information of real subjects that is personalized, then you still have to go through a research ethics board approval. And that's really rooted in Nuremberg and just wanting to stay away from obviously that the horrible ethical implications of scientific experimentation.

Now having said all that, not only is there a process, but there's an ethos. There is a culture of research and respect and confidentiality. And, first and foremost, understanding that harm can result. And I think that is the one piece where it has to be government industry, individual leaders within the sector that have to kind of come together and, yes, leverage the platforms you're referencing. But also create that that culture of care.

Jodi: Yeah, and that's something which is really difficult to do in such a decentralized industry where people get involved in many cases from a very early age. I mean, I've been programming since I was eight years old. And I think that it's really difficult to try and create a consistent culture across such a widespread base.

So you look at the way that medical schools function and the idea of taking the Hippocratic oath, and there are parallels in other industries. And one of the things that

this reminds me of is how Canada and Ontario in particular has a different view of the term engineer than the United States and many other countries do. Engineer is a protected term in Ontario, and if you studied computer science, at least when I studied it, you couldn't call yourself an engineer unless you had actually graduated from an engineering program and then became a professional engineer. Whereas in the United States, there are many 12 year-olds that call themselves software engineers.

And so that there are different standards that are associated with being part of a professional organization that simply are not part of the culture of software engineering as a whole throughout the world.

And so I think that building in that culture of security into software engineering or engineering overall, that's something that's going to take time.

Jodi: Absolutely. So let's talk about cyber security at a personal level, and the risks that an individual can bear as a result of even just using their phone. Now I'll start with a very dramatic example, and if you look at the case of Jamal Khashoggi, his conversations were monitored through a Canadian citizen, his communications with a Canadian citizen. And it was the Canadian citizen's phone that was compromised that created this portal to Khashoggi and rendered him a target.

So when we think about that that level of personal risk… So we started with the financial, which can very quickly also become personal risk and it can become economic risk, and then we talked about the geopolitical risk side of it when we see nation states and state actors leveraging cyber security and using it as a weapon as opposed to a defense. But what about that personal level of risk, that that's an example of a nation state getting involved. But how much risk do we all carry around in our pockets?

Shuman: It's a great example of that network effect of having many different parts of a technology stack that can each create the opportunity for vulnerabilities and compromises. So in the case of people communicating with each other over text or over email, I think one of the most obvious things that people often don't think about is that whenever you send a text message or send an email, there are two copies of that at least. There's what you send, and then there's the recipients inbox that now has the exact copy of the same content. And so either of those accounts can get compromised and the attacker is now going to have access to that data.

But there are many other points along that communication that could also create the opportunity for that data to be intercepted. So let's say that your email account wasn't compromised, your phone could still be compromised. The recipient's phone could still be compromised. The network which is used to be able to transmit that data could be compromised. Your home wi-fi router could be compromised.

You could have, as I said before, a completely unrelated hack on a system that has nothing to do with the recipient's email where the recipient has used the same password as they use for their email account that now allows their email account and your emails that you've sent them to be compromised.

So thinking through this network of interconnectedness is beyond the scope of any consumer to figure out how to be able to fully secure all of this data and all of these communications. And so instead what you need is that research kind of mentality like you were mentioning before in the context of the medical industry, where all technology providers are thinking about their interconnectedness and thinking of it through a security lens in order to be able to create systemic solutions that allow consumers to be protected by default.

So an example of this is the way that Apple has architected their text messaging systems where the communications are actually encrypted from end to end. So Apple doesn't have the ability to be able to retrieve that data. It's not stored in a cloud somewhere in a way that could be decrypted unless you had access to the accounts. It doesn't mean that it's not possible for the phones to be compromised or for the operating system to be compromised or for the accounts to be compromised, but it does mean that it's more secure than a system where there is a third party who has a way of being able to access that data as well.

And so there are other such systems that exist. You look at the way that modern web browsers communicate with web servers. And those communications are now encrypted in the end so that you don't have the ability for your internet service provider to be able to retrieve and spy on the websites that you're visiting or the data that you're sending to those websites.

Jodi: But if even Jeff Bezos can have his system compromised, how safe are we?

Shuman: Well, there are different levels of attack that I think disproportionately affect different segments of the population. So if you're Jeff Bezos or you're the President of the United States or the CEO or CIO of another public company, then you might be singled out and you are often singled out for compromise by a variety of different attackers. And so there are specific things that they need to think about in terms of information security, as well as physical security of course, in order to function in their roles.

But when you think about the average consumer, they often thought there's nothing special about me. There's no reason that I need to worry about security to the same extent. And that's definitely true from the perspective of cyber criminals don't care about the identity of an individual random consumer in the population. But technology now allows them to be able to target thousands or millions of those consumers at scale while not caring about them as individuals.

And what that means is that we are now bombarded with attacks constantly. So you look at the amount of spam that you get in your spam folder, you look at phishing emails that you get where someone might not know your name. They probably don't care about you as your individual identity, but they still want to steal your money and they're trying to fool you into falling for some scheme in order to be able to extract money from you.

And there are so many such schemes that are basically just numbers games. They're trying to send those initial emails out to millions of people around the world. Then a subset of those recipients are going to respond to the email, and then only a small subset of those are going to take the scheme to its end and actually send money to the criminals that are trying to steal from them.

And so if they can do that repeatedly and profitably, then they're just going to continue to engage in that behavior. And we have to think about how do we protect society as a whole against that instead of thinking about what do we do as individuals necessarily. And so how that translates to on an individual basis is greater education, greater thoughtfulness about what services and platforms do we use. What are their attitudes when it comes to security and privacy? And that ultimately, I think, translates into brand.

So when you've got companies that have a strong track record of investing in security and investing in privacy, those are going to benefit in the long term in terms of consumers who will say, I don't have the time to investigate the detailed security policies and practices of this particular company or any of the providers that I work with. But because other experts have said that this is a company with strong security practices, I'm going to give them my business.

Jodi: Shuman, the central question of this podcast is do you truly value something if you're not thinking about how you could lose it. What's your perspective?

Shuman: I think it's really difficult for people in general to place security or privacy at the top of their list of concerns in life or in any business transaction, unless they've had some kind of personal experience that illustrates for them the downside of not having security or privacy protected.

You look at identity theft, for example, and people behave very differently when they've been the victim of identity theft and they've been unable to get credit as a result of their identity being stolen than if that's simply something they've read about that affects somebody else.

It's fairly similar to the way that people think about their health and their diet before they've had some kind of a major health scare versus afterwards. And so I think that what we have the opportunity to do is create much greater education so that people

can learn from the bad experiences of others before they have to have that bad experience themselves.

Jodi: Shuman, thank you so much for spending time with me and for enriching us all and giving us our initial education lesson in cyber security. Appreciate it.

Shuman: Thank you so much, Jodi.

[Music]