# Cyber Security: The Backbone of a Successful Digital Economy

Mr Ashoke Baddage

*Country Manager, Check Point Software Technologies, Sri Lanka*

I'm going to talk about cyber security. What I would call the backbone of a successful digital economy. . I want to discuss national growth and digitalization at very high level and then what are the challenges we may come across along our way and then why cyber security is becoming the backbone of a successful digital economy? And what is our role? And then if you don't embark on a successful digital transformation. What will be the threats that we may face and the cost of such threats other? Breaches that is happening. I'm not an economist, but so the theme today is about the digital transformation aligned with the national growth as well. So what is national growth? So, we measure the increase of GDP or national input output over the last year. And if you look at the economic development, it is not just the growth of income, so that will be measured by the quality of life. How have we increased our living standard over time? Have our educational standards been increased? The public services that we obtained day-to-day have been increased, or whether it is at the same level. And have we improved our infrastructure and then whether the economic activities have been diversified into different areas and across society? And the most important factor in measuring economic development is whether you have increased your annual income. So per capita income, whether the distribution is equal between the rich and the poor. So now when we are talking about the national growth and digital economy. It is imperative that you know we must have a kind of technology introduced into. So basically, the economic growth is a subset I would say because of economic development of a country and it says we do not need to give much effort for growth because it happens naturally when there is economic development is happening. Everyone must develop an economy and contribute, especially if you look at it from the national level. The government should have the right policies in place with the right legal framework and provide the infrastructure needed. Development, especially when a digital economy. So, if you look at an economy today, so economy comprises of I would say. 5 pillars, right? So, you have your government on top and then your enterprises, businesses, manufacturers, entrepreneurs doing business on one side and on the left side, we have us the households. And we have the financial system in between to support this economy. And of course, we do trade between the countries, imports and exports. Business as well. So, what is growth? So, growth is when you and I increase our purchasing power when we have more money, we will buy more things, goods, and services. So, we buy from industry, the people who provide these things. So when we buy more so they also will get more income and then eventually what we do. We pay more taxes to the government. Right and the government responsibility is to provide us the required infrastructure

facilities for our growth. Now I extracted this from the ICT website. I'm not going to talk about it now, this is. The Sri Lanka government strategy. 4-4 years from 2020 to 2024, so they have given the architecture what they are going to do and responsibility and the stakeholders of everyone now. Here, what they are saying is they will provide the platform. They will provide the network between the government agencies, and they will provide the cloud. They will provide the cloud services also, and. Then interoperability platform along with the common database. So, this will be used by the different departments and ministries to give US service now.. For example, if I want to get my revenue license done so I go online and get it done. Right now I have two questions. Can I do it at any time? Is the system available and the 2nd is? Whether I'm exposing my data publicly, whether it is secure now? Those are the questions that we need. To ask. And,you can have a nice strategy. Implementing that depends on multiple factors. For you to do some homework, please look at this I CTS strategy and evaluate yourselves where we are today. Right? So when we talk about improving our productivity and digital transformation over the last two years, we have completely changed the way we live, work and learn. Because of the pandemic we were forced to do things that we never done. One of the key things is to increase work from home and then remote workforce. Now, many organizations were forced to let their employees work from home. Because they were locked downs and curfew, and people were unable to. Come to officers, officers to do their day-to-day work. Now, many organizations were not ready with the right infrastructure to provide that facility to employees. Now what are the challenges that we face working from home? First, you need stable connectivity. You need to connect to your office, cloud, applications, databases, and such. No, exactly your employee can access what you're supposed to do, right? I'm not going to each of these things, but if you look at everything has transformed over the last two years, predominantly not only in developing countries, even world over, so things are changing. Me enterprises are moving on to cloud. Why Professor Janet also mentioned? Because that will help you to bring down your costs because rather than maintaining your own network infrastructure, your own data centers can provide these services from the cloud service providers that will help you to reduce your costs. And at the same time. Ensure that up time or the availability is 99.9% because I mean if you look at the public clouds, those are. Those are large organizations like Glue, Google, Microsoft AWS and things like that, but there is a fundamental question. When you move your data and assets to the cloud. Is it secure? If it is in your premises, you know with controls you can secure, but when you move things to the cloud, how do we ensure? That our data is safe there. So that is another question. Now if you look at each of these things, security is a serious concern, online education, is it safe? I mean if you look at today's education and healthcare. Is big business And later, I will show you the data breaches which industries have been impacted most.t. Right now, when you do a digital transformation process. It's not a one-step process but must be phased out. If you do not carefully plan it out, you will end

up in disaster. Right, so I would say technology provides a stable platform in order to. Go towards digital transformation and why we need digital transformation. End of the day. Just because everybody else is doing it. and consumers. Drive the digital transformation on the organization because consumers like us. We want things to be better. We want to get our things done faster, secure, right so? Companies will be driven by these demands and obviously they will be pushed to do digital transformation and the fundamental thing is the underlying technology which provides a stable platform. But having said that security ensures a safe digital life for consumers.

Now moving from the enterprise world to the I would say international level now few years back if you look at. Between the countries, what did they do? If they have some issues, they go to war, right? They had a physical war, but now this has completely changed now. Now you would see what is happening in Russia and Ukraine. Go due to that. How it impacted, so I'll tell you some. Stories about how this cyber warfare is happening between the countries is no longer physical. You do not need guns to fire collapsed buildings and bring down an economy, so cybercrime is enough to do that. When we are moving to a digital transformation, the government's job is to provide the. Utility basic utilities to its citizens in a much better way. So, they need to introduce technology in delivering utilities like electricity, water, gas, transportation, healthcare, education, these things. So, you need to have digital platforms and if it is not secure, what will happen? Somebody can you know, hack into these networks, and bring down the entire thing and. The citizen will go completely, you know, blank. So, these things happened even recently when the gas lines were attacked, gas supply was blocked, and the countries during the winter have a huge, severe challenge. So let me tell you a story. Some time back Sony cooperation made a movie. Called the interview and basically the movie is about the North Korean president. And they portrayed a negative image of the president. So obviously North Korea didn't like it, so what did they do? They did not go into a physical war, they just brought down Sonic Operation Network and what is the impact to the economy of the US? So that impacted more than more than. I mean, I would say millions of Xbox users at that time, so this is the kind of warfare that is happening today and in Estonia. So they had a statue called Bronze Soldier, so this was before, you know, the. Separation when the Russian Federation was there. So once they separated, they what they did was they moved this statue from a very prominent place to very insignificant place near a symmetric so that Russia didn't like it because they value this statue a lot. So they what did they? They started attacking the government website. Estonian government website. They started attacking the media outlets and the entire banking system, so this is the warfare you see today. Also look at some of them. A major attack has happened recently, so we are talking about digital transformation. Now these companies that we are talking about have gone through these phases, right? So they have transformed, so they are providing better services through digitization to their customers. But still, they are. Attacked so we

will see why now the colonial. Pipeline attack that happened recently. Now the important thing here is that it was a ransom, so they attacked this company. And demanded ransom is millions of dollars so. The colonial pipeline decided to pay for it immediately, why? Because we did not have proper backup or recovery plan in place, there is no way that they will. They are going to continue their business operation, so they immediately paid. And I mentioned about the Russia attacking Ukraine and the other European countries. Many critical infrastructures. So like power, the gas supply, and things like that and then the Costa Rica County ransomware, again Russian attackers. So, they hacked into the country's financial system. Crippling the financial system. So why is this happening? Why is this happening now we said. Digital transformation is a carefully laid down process. Right, so you need to have your strategies in plan. Place the plans in place. And you are doing it investing millions of. Dollars or rupees and go to a digital transformation in order to provide. Efficient services to its stakeholders. The customers, right? And they have invested a lot of money. Then still. Things that I mentioned earlier is happening between countries cyber warfare. And criminals target the financial sector, the banks, and the enterprises. Still, it is happening. Is it because the securities solution providers companies like the company that I work for checkpoint? Which has more than 25 years of history specializing in security, right? Providing solutions. So there are many companies like that in the world. So are you trying to say that the bad guys are smarter than these companies? Why is it happening? It is not. So it is an integration of technology, the processors, and the people. Now if you don't have a tight integration between these three. There will be issues not only marching towards the digital transformation even after doing that. How to the sustainability of the same project, right? So you need to have these things together, so let me explain why. So as a technology platform we need to have our infrastructure ready, whether networks, whether it's a physical network, wireless virtual, whatever it is, and then you have your computing power and your storage and other old technologies in place. So, that is the first thing you provide. Right platform towards the digitization, right? And then you have. Your applications, databases, APIs, and things like that running on that platform. Your platform is ready, your applications are ready, and you are ready to serve your customers. So, this must be supported in every country. With the right legal framework, because when you move to digitize the way we work, it is also changing, so we need to change some of the laws as well. Simple example e-mail communication. I mean if it is not legal. Because these days we know that when we even go to a bank to, we throw money, we need to place our manual signature. Has anybody here done that? Can you please raise your hand? If anybody has signed some document and taken money do not think because right now we are using digital forms, right? It could be an ATM machine, Internet banking transferring to somebody else, mobile banking, all those. Right now, the legal system should support this digitization as well, and this is one of the key areas. And then finally we need a proper

security solution. Is 1 solution enough? No, I do not think so. If you look at the companies that I mentioned or the government that I mentioned, they have invested billions of dollars into their security system still bridged.

Right?

One thing is what we can do is together so we can raise the bar that hackers are trying hard, right? So that is from the technology perspective. That is what we are doing. We are raising the bar to block these hackers. But still they become successful. Because you need to have the right processes in place. And you need to make your people aware in the organization and you should have the right digitally skilled people in the workforce, and integrate technologies and ensure proper security in place. Now today, if you look at security, it is not just a simple solution, right? So we might need a different solution to protect your networks, whether it is wireless, wired, virtual, whatever. It is, right? So you need different technologies, and you need to have other different technologies to protect. Cloud because I said when you move your data into the cloud you don't know you don't see if somebody else's hand. So you need to have different technologies to protect the cloud. And applications the same story and more important, the end users because the end of the day. Most of the targets are happening through the end users. End users in the sense of the. Employees, if you look at the university network, it's you right. You have important content on your servers so. If you don't act responsive. It's a huge challenge. Whatever the technology we have in place. Whatever the processors that you have in your place and the people don't act responsibly, there will be a. Challenge so that is why the people factor is important and you have a huge role to play. Whatever you do, you even use your mobile phone. Right? The simple example is you know we. Are getting a. Lot of forwards, a lot of things that you know forward by different people with links and things like that. And emails so e-mail comes with attractive promotions. Click the link and provide you information. Those things right. So there are different ways of means. The attackers are trying. If we act responsibly, if you don't click the unknown and link if something that that is not sure best is done click. I mean whatever the technology. Sometimes I may not be able to help you. Now there are technologies. Having said that, if you look at the enterprise world, I mean there are technologies to protect the end device and users. The IoT and other huge, exposed area because I OT security is typical, we know when you talk about IoT it has become part of our day. Today life. I mean whatever device that we use, including the vehicles, the washing machine, the air conditioner, so all those things we can control remotely. And if those devices are not protected, again, those devices are controlled through the. Network end of the day, right? So the network is the platform for anything. So if you don't have the right security in place so you are in risk. And if you don't do that and throw these things away. To a basket, don't think about the right processes. Don't think about the right technology. Don't think about the training, your people and implementing a proper security strategy for the organization. This is the result, this research is recently done by IBM and they

say the largest compromises has happened through phishing attacks and. Business e-mail compromise. So end of the day both are the same, right? So these attacks have come through phishing and today most of the attacks I would say 80% of the attacks. Are coming through the fishing. So you need to have your right security in place. That's what I'm saying. One day when you go out and work for an organization. The number one fundamental thing is if it is an unknown e-mail, don't do anything because you don't need it. Right, I mean today there are multiple ways of communicating. So always you can cross check if there is anything important. Because the attacks that is happening today, it's exceedingly difficult for. Ordinary users to understand. So this is what I wanted to discuss with the time available. And end of the day. What is important is going towards growth nationally and individually and as an organization we need to embrace the digitization so when you do that, you need to have a. Very carefully laid plan. Things to consider when you have a digitization plan. Now I showed you the ICT plan strategy. The questions that I would ask you have a plan. Genuinely nice, nicely laid down plan. Do you have the resources to do that? Number one? Do you have? Do you have people? Do you have money to do that? If not, what is the point of having a fantastic document, right? Do we? Have people so. These are the questions that we need to answer and review the digitization plans like six months or one year time and see where we are. If something has gone wrong, then we need to identify what the things are. Whether we did not have money or something else. We didn't have. People understand those things and address those things. So what I'm saying is. It must be more practical. We can lay down processes. I have been tried and tested by large organizations but having said that end of the day things needs to be practical so those things you need to. Properly identify and work accordingly, and if you do that, you have a successful. Digitization program in any enterprise. And at the end of the day again, I would say you can have a kind of a nice platform to drive your digitization efforts, but. Cybersecurity is the backbone of a successful digital economy. Because if you don't have the right security in place, it can collapse at any moment. With a single attack single malware.

Thank you!