Globalization and cybersecurity trends for the future are expected to evolve in the following ways:

* With the continued growth of globalization, there will be an increasing interconnection between nations, businesses, and individuals. This will lead to an increase in cross-border cyberattacks and cybercrime.

This is because cybercriminals can exploit vulnerabilities in interconnected systems to gain unauthorized access to sensitive data or disrupt critical infrastructure.

In addition, as businesses and individuals become more reliant on digital technologies and cloud-based services, they become more vulnerable to cybercrime. For example, an attack on a cloud-based service provider could potentially affect millions of users around the world, even if they are located in different countries.

In summary, the trend towards greater interconnectivity is expected to continue in the future, but organizations and governments will need to be proactive in managing the associated cybersecurity risks, invest in cybersecurity training and education, and collaborate with other organizations and governments to share information and best practices.

* Cybersecurity is expected to become more automated with the adoption of artificial intelligence (AI) and machine learning (ML) technologies, allowing organizations to detect and respond to threats more quickly and effectively. By automating these tasks, cybersecurity professionals can focus on more complex and strategic tasks, such as developing and implementing security policies and procedures.

However, it's important to note that while AI and ML can improve cybersecurity, they are not a panacea. These technologies can be vulnerable to cyber attacks themselves, and they require ongoing monitoring and maintenance to ensure their effectiveness.

* The rise of IoT devices and the interconnectedness of systems will continue to pose a significant cybersecurity risk. As the number of connected devices increases, so too will the potential for cyberattacks.

(The Internet of Things (IoT) is a network of interconnected physical devices that communicate with each other and with the internet. These devices can include everything from smart home devices and wearable technology to industrial control systems and medical devices.)

Some of the key IoT cybersecurity trends to watch in the future include:

* + Greater focus on securing IoT devices
  + Use of artificial intelligence and machine learning
  + Adoption of blockchain technology: Blockchain can be used to secure data and transactions in IoT networks, making them less vulnerable to cyber attacks.
  + Increased regulation
* The adoption of cloud computing is expected to continue to rise, but this will also lead to an increased risk of data breaches and cyberattacks targeting cloud infrastructure and data.

A single security breach can potentially impact multiple organizations. As a result, cybersecurity professionals and organizations need to focus on securing cloud-based systems and data. This includes implementing strong access controls, monitoring for unauthorized activity, and implementing encryption and other security measures to protect sensitive data.

* And another one that is very new and will continue to grow is the notion of a deepfake. That is an audio or video file where we have a a person, maybe a well-known person saying something that they never said. And we tend to believe what we see. And if it goes out on social media, everyone will believe it before anyone has a chance to refute it. It could also move the stock market. If we had a CEO seeming to say certain information that would look bad about the company and cause the stock to crash, even though they never said those words, but we have an AI that can do that sort of simulation. We're going to have to get smarter about how to detect a deepfake from an authentic video as an example.
* Quantum computers are very useful in solving problems that traditional computers have not been able to do. Also, a quantum system could potentially attack the cryptography that we have. The asymmetric crypto algorithms that we rely on every day for all of our secure communications could potentially be broken in what we thought would have taken decades or hundreds of years. Now, with a well-tuned quantum system in the future, maybe being able to be broken in a matter of minutes. So that means we're going to have to do some good work to make quantum-safe algorithms for cryptography. And the good news is we've got these things. In fact, the National Institute of Standards recently this year came out with four algorithms that they published as being quantum-safe.
* Cybersecurity skills shortage: The demand for cybersecurity professionals is expected to increase as cyber threats continue to grow, but there is a shortage of skilled workers in this field. This could lead to increased outsourcing of cybersecurity services and reliance on automation and AI.
* Cyber warfare: The potential for nation-states to use cyber warfare as a means of attacking each other is expected to increase, leading to a greater focus on national cybersecurity strategies and defense.

Overall, the future of globalization and cybersecurity will continue to be shaped by new technologies and emerging threats, and organizations will need to remain vigilant and proactive in protecting their systems and data.

**Video subtitles**

What can we look forward to in the cybersecurity? I think there will be both good and bad news. So first of all, one of the things that continues to plague us is this notion of data breach.  That is the hackers get into system, dump customer database and use it to mine for information that they can later use identity fraud scenarios with.

And ransomware is costing people, individuals, all the way up to the large organizations and even nation states. As its effect is resulting in data loss, it's resulting in extortion. A lot of bad things happen here. So those are a couple of bad trends that we see. How about something good, a little bit of good news for last year? I'll say multi-factor authentication is one. It's not a new idea, but the idea that I can authenticate, prove my identity to the system based upon something I know, something I have, and something I am. Those three things put all of those together or some combination. Maybe even get rid of the something. I know the password. It's a better user experience and it can lead to better security. And what we've seen is more and more widespread adoption of multi-factor authentication. That's going to be a good thing for us all. And we've seen that start to take more hold in the past year. Now, how about looking forward? What kind of things have can we expect to see? Well,  I'm going to say it's going to be a little bit of Groundhog Day. What we've seen in the past, we're going to keep seeing in the future until we learn how to solve these problems. Data breach, ransomware, multi-factor authentication. Hopefully, we'll continue to see more and more widespread use of that. So the past continues to play into the future and influence the future,  but what are some other things that we'll see?

I think we're going to see a rise in attacks for  Internet of Things. Internet of Things, or IoT, is basically the notion, if you follow along with me,  turn everything into a computer-- your car becomes a computer that takes you places.  Your refrigerator is a computer. It keeps your food cold. Your DVR is a computer that shows you  movies. And in the IoT trend, everything becomes a computer. And what we know from cybersecurity  is that every computer can be hacked. So if everything can be a computer and every computer  can be hacked, all of a sudden everything can be hacked. Your car, your refrigerator,  your insulin pump, your implantable defibrillator. These are things that are going to be pretty scary  when we start thinking about the whole world around us is potentially hackable. That's an  area that we have got to give more attention to.

Another one that could come back to haunt us is  the use of artificial intelligence by the bad guys. On the positive side, we've had the good  guys using AI for some number of years. We can use this to do a better job of security analysis,  of root cause analysis, looking for what all of these indicators of compromise ultimately mean,  and figuring out what we need to do. The good guys are using this to analyze and investigate. The bad  guys, I think are going to start using it more and more to do things like develop attacks that are  specific to an AI.

An artificial intelligence system would be able to maybe design new types  of attacks to get into systems. We could also, as our businesses become more and more dependent upon  artificial intelligence, we are dependent upon the corpus of knowledge that's in those systems.  So therefore, if someone were able to poison the corpus of knowledge, then the AI would be  giving advice and making decisions based on bad information. So that's a different type  of AI-based attack. All of these go into what we refer to as adversarial AI. So there are a  number of things that the bad guys could be doing where they're going to start using AI more,  which just means the good guys are going to have to start using our AI more still.

And another  one that is very new and will continue to grow is the notion of a deepfake. That is an audio  or video file where we have a a person, maybe a well-known person saying something that they  never said. And we tend to believe what we see. And if it goes out on social media, everyone will  believe it before anyone has a chance to refute it. Imagine what happens if a video is leaked on  Election Day showing a candidate saying something that they never said that was terrible. It could  be too late before we get the news cycle-- the next news cycle ---to correct the error. It could also  move the stock market. If we had a CEO seeming to say certain information that would look bad about  the company and cause the stock to crash, even though they never said those words, but we have  an AI that can do that sort of simulation. We're going to have to get smarter about how to detect a  deepfake from an authentic video as an example.

Other things that we'll see. Quantum computers  are very useful in solving problems that traditional computers have not been able to do.   To do simulations and things of that sort, that we just don't have the computing capacity to  process with a conventional computer. So a quantum system could solve those problems in record time.  Also, a quantum system could potentially attack the cryptography that we have. The asymmetric  crypto algorithms that we rely on every day for all of our secure communications could  potentially be broken in what we thought would have taken decades or hundreds of years. Now, with  a well-tuned quantum system in the future, maybe being able to be broken in a matter of minutes.  So that means we're going to have to do some good work to make quantum-safe algorithms for  cryptography. And the good news is we've got these things. In fact, the National Institute  of Standards recently this year came out with four algorithms that they published as being  quantum-safe. These are the algorithms that will protect against a quantum computer trying to crack  our encrypted messages and databases and the like. And four of those algorithms that were accepted, of those four, three of them, in fact, had IBM contributions to them. So we're very proud of  our work that we've done in this space in trying to protect people going forward into the future.

And then another trend that has continued for a number of years and it shows no signs of letting  up is a skills gap in cybersecurity. There's one website called cyberseek.org that says, currently,  as I look at the website, there are about 770 million unfilled cybersecurity jobs in the US  alone. That's right now, and there's only about a million or so people working in the field. So  it's almost 1 to 1 for every job. Now there is an opening and we can't make cybersecurity experts  that quickly. With current technology, we can create a new human in about nine months. But if  we're going to turn them into a cybersecurity expert, it's going to take a few more years.  There's not anything that looks like we can suddenly start minting new cybersecurity experts  to fill the gap. But we can do some things to help. And we can do things by working smarter  using AI that I mentioned here to guide our security efforts, using good tools to automate the  responses that we have for security, to do better analysis and become force multipliers for the  people that we do have. Also, we need to do a lot more training for the people that are out there,  not only our end users, so that they don't put us in such a bad place to begin with,  but also security professionals and create more security professionals. So it's going  to be a multi-pronged approach, but these are the things that I think we're going to be able to see,  both on the positive and the negative as we start looking forward to the future of cybersecurity.