FRAUD TALK – EPISODE 101

The Rise of Cybercrime During COVID-19

In this episode of *Fraud Talk*, Arpinder Singh, CFE, partner and head of India and emerging markets, Forensic & Integrity Services at EY, highlights how cybercrimes like business email compromise (BEC) scams, phishing and account takeover have risen and will continue to rise over the next year.

Transcript

Mandy Moody: Thank you for joining us today for another episode of the ACFE's *Fraud Talk* podcast. Today I am joined by Arpinder Singh. He is based out of India's EY's Forensic and Integrity Services. He's a partner and head of India in emerging markets there. Arpinder, thank you so much for joining us today.

Arpinder Singh: Thank you so much, Mandy, for having me here today.

Mandy: I'm excited to have Arpinder here. We're going to talk a little bit about cybercrime and what we're seeing happen right now with cybercrime during COVID-19. First, Arpinder, tell us a little bit about you, and what you do at EY, and some of your main responsibilities there.

Arpinder: Thank you so much, Mandy, for this. I head the forensic team in India for EY. I also head the forensic team in the emerging markets for EY. I also sit on the Global Board Forensic, which is a steering committee.

Besides this as a profession, I'm a chartered accountant and lawyer by education. I've been a finance controller in the U.S. I worked for many years in the Bay Area as a finance controller until I moved back to India and started forensic accounting many, many years back, when in India, there was nothing called fraud. That's what happened when corportations or clients, and you said, "You have a fraud investigation," and they'd say, "What is fraud?

I started long, long back when forensic was still a very new concept in India. I was very lucky to have started at that time. It's been a great journey, as I've done internal audit, strategy audit, and then spent the last 16 years just doing specialized forensic work in India.

Mandy: You've been around before there was fraud?

Arpinder: That's what they say in India. It's been a great journey. I set up the ACFE chapter in Mumbai, a founder of it. ISO 37001 came in on writing corruption. There's been a lot of changes every year in India, which I would love to discuss with you as we continue this conversation.

Mandy: Let's dig into COVID-19 and the coronavirus and how we've seen fraud change. There is no illusion that fraud has increased. We've done our own surveys here, and I'm sure you've seen it happen as well in what you're dealing with. The fraudsters and people who are out to game the systems use these times, these vulnerable times, to really, really go for it.

One of the areas that's definitely been affected is cybercrime. We know the risk has increased, and the exposure has increased. Why do you think it is increasing now? What are the ways that you're seeing it play out?

Arpinder: I think the first and biggest thing is everybody was unprepared. Let's be honest. I think everybody has business continuity plans, Mandy, but reality is those business continuity plans have never been tested to the extent the pandemic has tested it. None of us, in my life, I've never sat at home for six months, which we've been doing, and working from home for six months. I think when it hit everybody, I don't think any company or corporation was prepared for it.

What I saw in India was a little crazy. You had companies which were sending computers and desktops back to homes in the back of a car. There were trucks being hired, which were uprooting computers and infrastructure and sending it to different employees' homes. No one was fully prepared for this type of a pandemic and how long it's lasted out.

I think, first is the business continuity plans have been fully tested. Obviously, there are large corporations, which may have been slightly better prepared and have better infrastructural resources to deal with it. The mid-cap companies, and the smaller companies obviously would never have dreamed of something like this, and with the infrastructure to support it. That's the first.

Second is…let's take “work from home.” You have employees who have had to deal with not having great Wi-Fi connections at home, or not having great connectivity. Maybe they were dialing it from their phones. Companies had to open up their firewalls to allow people to work from home. There's always a gap, right? It takes maybe a week to set up a firewall, or let's say employees had Bring Your Own Devices where they were working from home.

Suddenly, the whole system and infrastructure and computer networks that I saw during this pandemic had been fully tested. I don't think companies, as I said, were fully prepared for it.

Let's give an example. You have a large company having a lot of personal, confidential information in the computer. When you're working in office, there are rules which say you cannot take a camera shot, or take a copy of that personal information from the computer. When now the employee has access to their personal information on their screen at home, the only thing which is stopping them from stealing that information or exposing it to a hacker is your personal integrity. There is no way a manager can come to your house and sit on top of you to make sure that you're not taking a snap using your cellphone. That is a risk.

Second is dialing in through Wi-Fi mobile connections onto your computer networks. Hackers are very smart.

They're far ahead of us, which is why they have their cyber cases in the world. They're going to get into your networks. That's the second thing in my mind.

Third is the amount of internet transactions everyone's doing. You can no longer go to a Walmart, for instance, in the U.S., or stores in India. You have to buy online. That means everyone is sharing the credit cards. People aren't just sharing credit cards with reputed companies. You're trying to buy boutique stuff. Someone's trying to say, "Hey, we got this fantastic herbal medicine for COVID. You have this five times as a day and you're going to be all fine." You're going to click on that because you're desperate.

Hackers are working on people's desperation. You can easily send you an email, Mandy. If it's interesting enough, telling you a little bit about COVID, or telling you about a new vaccine which is coming out in a different part of the world, you will click on it. I think hackers have a perfect time. If you ask me, the pandemic has been a perfect environment for them.

When people are desperate, people are emotionally stressed. Everyone's online. People are shopping, maybe 80% more online than they ever did prior to the pandemic. People are logging into networks working from home.

Let's say now…I'll give you an example. We have an issue with a client with a Bring Your Own Device. The question is, if you have an issue with a Bring Your Own Device, you can no longer have an engineer who goes to a remote location in India and fixes it. Suddenly, this employee has malware on his computer, and he's still logging into your network. It's going to get exposed.

Let's say you have old routers or an old server from an infrastructure perspective. You can't go and change it. It's like doing your renovation in your house. You got to postpone it. You want to say, "When the vaccine comes out next year, we'll get my renovation done then." Same way is with the computer network. Until it doesn't hit you, you're deferring these decisions, and that's exposing you.

I can take the whole session talking about this, but, Mandy, the pandemic has exposed us to risks we could not even imagine.

Mandy: What can companies do? I said I was going to ask you about a cyber incident response plan and why it's so important. Is that the place to start? Is that where you invest your time and your money?

Arpinder: I would say that's very important. You're going to have big companies, small companies, medium companies. You're also going to have companies which have not so much personal data. You're a real estate company, for instance. You're doing construction of roads. Would there be so much personal information? Can a hacker really destroy them? Maybe not.

You have an IT company which is servicing global clients. Could a hacker impact them significantly? Of course. One is you have size of companies where they can invest in it. Second is type of companies based on the exposure.

I think a cyber incident response plan is extremely important. If you've not assessed your risk, and you've not planned for it considering the sector you work in, the type of information you have, the infrastructure you have, you're going to be heavily exposed.

I think you're actually right. I would say companies who have, in fact, been impacted or not been impacted, lucky not to be impacted, should immediately start working on a cyber incident response plan. See their infrastructure, see where the vulnerabilities are, do a pen test, as we call it, where you can go outside to test a network to see if there are any cyber exposures. That is, I think, the most important thing to start with. If you don't start with a planned approach, and you start randomly, it won't really help. It is very important.

Mandy: I think what you said is, a lot of companies are reacting right now. They're in the reactive state of, "Okay, now, what do I do? We didn't see this pandemic coming, now we got to put something together." What are some ways that you think they can be proactive, moving forward?

Arpinder: I think the first thing is they should first map out their infrastructure, see where their vulnerabilities are. The first thing I did was tell clients, at least, is please check your network to make sure all your software is updated. A lot of people took shortcuts. I know software is not cheap, neither do I own any software company, unfortunately, Mandy, but reality is that people don't upgrade their [unintelligible]. They don't upgrade the [unintelligible]. The software is outdated.

They should first quickly check their hardware and software to make sure, is everything up to date? Is there any weak spot that a particular hacker could look at? That's the biggest vulnerability. You have pirated software, all outdated software, unmaintained software, or you have a router sitting somewhere in your network which is an old version, an old switch, or an old server. That's probably our biggest vulnerability, so, first, getting a handle very quickly around what your entry points are.

It's like a house. Where are the doors? Very quickly assess that. I think the second is, as you're assessing that, keep working on the cyber response plan, but don't wait because you don't have time, unfortunately. Assess your infrastructure. In parallel, start working on the cyber response plan. See what you can put in place because that's very, very important.

Third is, as a part of the cyber response plan, Mandy, start looking at what data do you have which is vulnerable. What are your critical systems? Your financial system, maybe, your system which has employee information, whatever your system currently which is critical for running your organization. Do you have an enterprise resource planning (ERP) system which is running your factories, your office? Is that critical for you? You need to protect that. Maybe, you create a backup for that. Maybe have two disjointed servers or networks which have the same system, which could be a backup. That's just an example.

Basically, you have to start assessing your infrastructure. You need to start working on the cyber response plan. You need to start working on backups. All these have to be done in parallel because, unfortunately, you don't have the luxury of a pre-COVID time saying, "We have a two-year plan. In two years, we're going to get to this level." You need to do it very, very quickly.

You need to risk assess on what is critical. You can't get everything in place immediately. As I say, protect your critical infrastructure. Protect your critical systems. Protect data which, if leaked out, can be very embarrassing to you, can potentially be a GDPR issue legally, or it could be a violation of some U.S. or Indian law. Start protecting yourself around that.

Also, start working on your skills and resources. You have the right people, you have the right training, you have the right people in your organization. Most companies generally are using maybe a mom-and-pop scanner tool for checking vulnerabilities. Get the best. This is not the time to compromise and be penny wise and pound foolish.

Mandy: Do you see the initiative being led by the top, from the CEO? Do you see it coming from the IT department? Do you see people coming together to say this is important? Where do you like to see, and see the most success at companies of where this message comes from and where this need to do it comes from?

Interviewee: I will break it into two parts, at least the way I see it, Mandy. You have companies which are more technologically advanced like the IT, ITS companies. I think their cyber is the agenda of the CEO. It comes right from the top. They realize the criticality of it. They have signed contracts with global clients where they have said data privacy is important. For instance, when there's an incident, you have to report it within X amount of time. There are very strict regulations around it, strict liability to them. If there's a violation, obviously, you can lose important customer. I think they're a little bit more advanced where it comes from the top. A lot of investment also goes into cyber infrastructure, and they're faster and reactive.

The second bunch are people who don't really have any external pressure, at this point in time, to do the right thing on cyber. There, I find, it's generally a Chief Information Officer (CIO) who will be dealing with the mandate. Personally, I don't think that's the right answer because the CIO has restricted budgets. If he doesn't have the tone at the top from the CEO giving him the right budgets, making sure it's a focus area, he is vulnerable. I would say the second bunch where there is no external pressure from a contractual perspective to ensure there's best cyber infrastructure, those people are the most vulnerable.

The time when they get hit with a ransomware attack and their systems which are running their factories, or the system which are running their financial system suddenly get blocked, there's a ransomware attack and a lot of them have happened in India and globally in the last six months, then suddenly, they wake up and it becomes a CEO agenda.

Unfortunately, that's reactive where suddenly now your company can't operate; you don't have an IT system, your data is all locked. You have a hacker who's saying, "You've got to give me X number of Bitcoins," which is definitely not legal, and then you have a demand and you start breaking up. That's too late.

In my view, this has to be a CEO agenda, no matter what type of company it is. Today, I think risks have moved from a normal fraud kickback type of risk to a cyber risk. Cyber should be the top risk during this pandemic, in the near future, and in the beyond, because technology is here to stay, Mandy. Everything has changed in our lives. Everything is going to be now technology-based. Cyber is going to be your biggest risk.

Mandy: That's really, really, really great advice. I want to move on to what companies are seeing right now. What are some of the current schemes that you've noticed and that you've seen?

Interviewee: I would say we've seen many, many schemes. The first traditional one is a CFO getting an email, for instance, from a CEO, saying, "Hey, transfer $500,000 to an account in Singapore. My account has changed and this is the new account number. Please do it immediately. I'm not well. I'm sitting at home. Please make sure it's done by end of day." The CFO gets —

Mandy: The business email compromise, yes.

Interviewee: The business email compromise. It's very standard. A lot of those are happening. I've done a lot of those investigations. It continues to happen as an issue. I think it's something most companies should be trained and aware of.

The second type of scheme I'm seeing is normal phishing emails, Mandy. I believe there was a survey done by an external company where India gets the largest number of these phishing and malware emails in the world. Obviously, we have the largest population. We have the largest number of COVID cases, unfortunately, going forward. The fact is we've also got the largest number of emails, phishing emails. I think it's going to be increasing.

Unfortunately, people are not empathetic even during the COVID times. Robbers, hackers are the same. They're sending emails around charity. For instance, if somebody wants to help a hospital, or somebody wants to help COVID patients who don't have food, they're sending emails saying, "Please, click on this. This person is dying. He needs some money to the hospital for the care."

People are pretty empathetic during this time, so you're clicking on that email, and that's when your computer gets compromised, or you're sending money, potentially, to an account which is a hacker's account and it disappears. The money goes through layers outside India and you can't trace them beyond a point of time.

In the recent pandemic, people are using unfortunate situations around the coronavirus to potentially either penetrate your system, penetrate your network, or even get you to spend money and put it in an account which, at a later date, cannot be traced. That's the second thing which I'm seeing.

Third is very sophisticated hackers actually freezing parts of an infrastructure of a company or in fact, the complete infrastructure of a company. A lot of them are publicly mentioned where portions of large global companies are frozen. They can't work. There are ransoms. You have to actually pay Bitcoins.

I've done a lot of those smaller cases, and finally seeing these bigger cases where you have Bitcoins being demanded, it's pretty interesting. I always thought it was a John Grisham book, but it's actually happening a lot as we talk.

Another thing I would say, these are small cases. That's also very important because those are dire. A lot of people are now being…for instance, there's attrition. People are being laid off, which, if you and I are having a call and we say, "Mandy, it's been great, but we don't have a business anymore." People are no longer meeting. There is no transfer of data happening. You have your office computer; no one's going there to pick it up. It's just lying there.

They're disconnecting their network. The handoffs are not happening with IT, which are clean. Confidential data of the company could be potentially compromised at that time because you have employees who have confidential company assets, data which is not being properly managed. I think that's a big issue which we have seen during the pandemic.

Lastly, I would say, is people are trying to make it easy for employees' ease of business. They're talking about contactless sales, contactless purchases, contactless this. It's a kinda cool thing to say. Obviously, I'm a little bit older than all of this, but what I see in contactless is everything now on cell phones, mobile, apps. You're making it convenient, which is great, but convenience without brakes, it's like getting this big luxury car without brakes, and you're going to have a potential pitfall.

Just some numbers, Mandy, if I can just quote some numbers. I find this quite interesting [inaudible].

We find that companies have faced more than 20,000 cyberattacks per day since May 2020. That's huge. The number of attacks has significantly increased per day. Over 94% of the attacks which were recorded were phishing attacks. Phishing is the largest scheme which is obviously hitting people.

Also, we found that organizations were not prepared. 55% of the people polled did not make protecting part of their strategy. The proactive cyber response plan was not a part of this strategy.

India, unfortunately, were ranked first globally with the highest number of detected spams. We have the largest number of people penetrating. Also, if you look at it, what we found is that one-fifth of the global respondents suffered a major cybersecurity breach, which is pretty high. If 20%, 25% of the people have suffered a cybersecurity breach, you have a pretty serious issue.

These are just some statistics, but I thought they're interesting to show how serious the issue and incident has become. It is better to catch the issue upfront rather than waiting for 12 to 18 months, when the issue is slightly out of control, you can't manage it and it becomes a global incident.

Mandy: That's from an EY survey?

Arpinder: That's right.

Mandy: I'm going to get that link from you later.

Arpinder: All right.

Mandy: Just to wrap up, what do you predict for the rest of this year and into next year? What are some top risk or top actions that companies need to take to be prepared?

Arpinder: That's a great question, Mandy. Before I answer that, what they have to do, maybe I can…We did a collation of what the different predictions on cybercrime are. Maybe I can take a minute on that.

I think that cybercrime damages are expected to cost the world more than $6 trillion is one of the surveys which came out. Maybe they were a little fatalistic? The fact is, it's going to be a big number. They say that businesses in 2021 will fall victim to ransomware attacks every 11 seconds. There'll be some company in the world, which will, unfortunately, be exposed to it.

There are going to be targeted social attacks using bots. For instance, I recently had a friend who came and approached me and said somebody hacked his credit card. Over two minutes, he suddenly got…it was like artificial intelligence and robotics, where he kept getting things every second. He lost, I think, $20,000 in a matter of two minutes before he had a chance to even call up the bank and close it. Artificial intelligence and bots are something hackers are going to be good at using.

What do I think about companies? Mandy, I would recommend companies should pause, work on the strategy, the response plan. I think they should also relook at their budgets. I know companies are struggling with budgets, and it's not easy.

If you have 100 risks you're looking at, maybe those 60 risks can be put aside, and maybe some part of that budget can be allocated towards cyber. Cyber, with the amount of technology being used, I think that is your biggest risk. I think that prioritization needs to be done by a CEO or someone at the top management or the board.

Once that investment is done, it's up to the CIO, and CEO, the C-level people, to come up with a robust plan, a pragmatic plan, and start mitigating the risks, and start tightening their circle. It's like COVID. You can say, "It's not hit me," but you never know when it does. Cyber issues are that. It's not hit you today, and you can joke about it, read the newspaper, but if it hits you tomorrow it's not going to be fun. Start working on the response plan. Start working on the budgets. Start buying stuff. Start doing it as we talk. Get the right skill sets.

Last, I would say training of employees. Mandy, the poorest thing I've seen is people are not training employees. Start training people like me, or you, or somebody, saying, "Don't click on that email. Don't get tempted. Don't share your password with your children. Don't open your computer and leave it on when you're working from home because somebody is going to come and do something. If you've got malware on your computer, please don't go to some internet site and start downloading some movies, which you're not allowed to because it will compromise your network. Don't go to some mom-and-pop store and buy a cheap software just because it's cheaper than an authorized software."

Some basic trainings, Mandy, are really required for the people when they're in corporations. Companies could do more than this.

Mandy: Yes. Wonderful. Thank you so much for joining us today.

Arpinder: Oh, thank you so much, Mandy. Thank you for having me.

Mandy: This is great information. Thank you so much for joining us, and thanks for giving us a little insight into what you're seeing. I hope you stay well.

Thank you all so much for listening today to *Fraud Talk*. We are excited to be keeping this podcast alive and well, even during a pandemic. We will talk to you again next month.