Business901
Building Funnels of Opportunity

CyberSecurity with Keatron Evans

Note: This is a transcription of an interview. It has not gone through a professional editing process and may contain grammatical errors or incorrect formatting.

Transcription of Interview

Joe Dager: Welcome everyone. This is Joe Dager, the host of the Business901 podcast. With me today is Keatron Evans. He is managing partner at KM CyberSecurity, a global information security consulting business which includes penetration testing, incident response, management and consulting, digital forensic and training. Keatron is also a senior security advisor at Savvius and a top-rated instructor for EC-Council and ISACA. He is also one of the authors of *Chained-Exploits: Advanced Hacking Attacks From Start to Finish*, a textbook still used by the US government security agency. Keatron, thanks for joining me today.

Keatron Evans: Thank you for having me, Joe.

Joe Dager: You've been in CyberSecurity for a long time, do you remember how you got started, was it even called cybersecurity back then?

Keatron Evans: It was not called cybersecurity back then. Nobody really called it anything. It was just one of those weird IT things that were kind of buried amongst all the other things that IT and computer people did. So there wasn't really a CyberSecurity, and there wasn't really a security associated with computers when I got started, but the way I got started; I was this very curious really early on, so I was actually doing hacking activities and doing things like exploiting systems before I even figured out that's what I was doing.

It all started as I was growing up in Mississippi, grew up in a very large family. My dad you know didn't make a lot of money so we couldn't afford things. What happened is I was able to give myself internet access by taking the little net zero free 30 days CDs that they used to send out and I would get those things and give myself free thirty days on like a library computer or somewhere like that, and I figured out how to very early on to get into the net-zero servers, get a list of all the accounts of everyone in the world that use net zero, so I was able just to hop around picking account and use it to give myself access, just you know until I was able to afford it or come up with other ways to get it and of course back then there weren't any laws against it. Like they couldn't… nobody could come after you or anything like that. They would just say hey we noticed that you were doing this, stop it. So I was actually very early on hacking as a kid, then I just didn't know what it was called.

Joe Dager: Well that's kind of scary that you could even do that back then with you know very little training, right?

Keatron Evans: A natural proclivity to find out how things work I guess.

Joe Dager: What's really changed in all these years? You said the laws weren't around back then, I know there is a totally different web now but really have the basics changed? Are there still people that just as inquisitive like you and try to break in and give some more access?

Keatron Evans: There are definitely still people like that, but some big changes that have happened are if you look at the last twenty years we've evolved as to how much information we put on computers and how much information we send across the computers. The whole concept of cyber-crime has evolved with that. The criminals are doing the things that they did before we even had computers, it's just that now the information and the data that they want are on computers. So computers now become victims and tools of the crimes.

What happened is when I started in the industry being a security person it was rarely even heard of. Now it's turned into this big industry because as more data ended up connected and as more data ended up on the internet there were more breaches. People needed to protect that data more that turned out to be a huge need for people with technical security skills. As a result of that the industry kind of started to take off. I was lucky enough to be one of the people that were in the industry very early on and that allowed me to get a lot of headway and became a little bit of being in the right place at the right time. So that was a big part of it.

Joe Dager: Timing is everything, isn't it?

Keatron Evans: Yes, absolutely. The other half is the demand. All of a sudden there was money involved in CyberSecurity, and if you have these skills, you can go and make lots of money. The word got around, so now everybody that knew anything about computers are trying to get into CyberSecurity now. Just to give you a point of reference when I taught my first ethical hacking class all the way back in 2003 the class would be made up of people that had at least 10 years of IT experience. The people that were in IT for a while and they were coming in to learn this security and this hacking thing. Well now my average class, there is usually maybe one or two people out of twenty that have even more than two years' experience in IT, and most of them have zero experience in security. A lot of the fundamentals of the networking, fundamentals of how memory works and all of these things, I have to teach that in classes now. Whereas back then that stuff was just common knowledge.

This just shows you how the industry has evolved and it is in very high demand things, and so now you have an influx of people coming in. Some of them without any technical background trying to elevate themselves really quickly into it. That led to a lot of demands for not just a consulting, but training as well.

Joe Dager: We always think that there is this powerful stake like the Russians hacking you know the Democratic National Party but why does the average business need to understand CyberSecurity? I mean so what, people aren't after my manufacturing data, are they?

Keatron Evans: Well they are. Actually one of the things that's changed as well over the years is if you look at China for example and some of the other threats. China actually has a stated mission. The government has a stated and documented mission to basically steal as much intellectual property from us and other developed countries as they possibly can. They actually have a coordinated mission, and they have money behind it. They actually have a division of their military whose mission it is to actually steal as much information as they can from the US and other companies. This includes things that we consider to be as normal manufacturing information and things like that because even with manufacturing there are trade secrets. There is intellectual property that the manufacturing company wouldn't want their competitors to know as far as how they do this process or how they get certain types of business.

Those things are definitely targets and more importantly than that what happens is you as manufacturing… let's say you are a small manufacturing company. You might end up being a proxy or a pawn for a threat agent to attack a government official or a government organization for example. They will use your network and your computing devices as pawns so that when the government does their forensics, it looks like you did the attack. So that's one thing that smaller companies or people say oh, they are not after my data. Maybe not but you have resources and those resources are just the channel that they can hop into and use to attack other places and kind of mask their identity via you. That's definitely another thing that you have to be concerned with as well.

And if you are a public company, you have regulations where you have to be worried about CyberSecurity because if your data gets stolen and it causes the price of that company's share drop. The shareholders have a libel suit against you because now you are responsible legally for maintaining some level of security, and this goes for hospitals and health insurance places. They have something called HIPPA. That's a regulation that says that basically if you have medical information you are responsible for securing it.

Same for any business that takes credit cards as a form of payment, there is something called PCI. That's a regulatory thing that requires you to maintain a certain level of cybersecurity to be able to take credit cards. It's becoming a very regulated thing. If you think about the recent grilling of Mark Zuckerberg with Congress when they had that committee to grill him. The Equifax breach that happened last year is probably one of the biggest in history. There is an entire congressional hearing about that breach, and they were the CEO, and some other people have to answer some really tough questions about why they didn't have these controls in place.

I think everybody has to be worried about it to some extent. Some places more than others but everybody has kind of responsibility now to do something.

Joe Dager: You really brought up two different questions for me that I thought about, one is that being that pawn; that's a lot about what's your original book was about, Chained Exploits. There is just a chain going on, a method. It's kind of like a mind map, a concept map of how someone actually gets compromised?

Keatron Evans: That's absolutely what it was about, sure and that's one of the big things that's a good connect there.

Joe Dager: The other thing that you bring up is that when you talk about government regulations, the first thing that jumps to my mind is we have OSHA inspections for safety and health, are we that far away from having data inspections that we have to meet and get reported? Is there something like that out in the future or is it now and I don't even know it?

Keatron Evans: Well its closer to its now and you don’t know it. There was recently something that’s was an international thing called GDPR. That was mostly steer headed by Europeans, but it’s affecting us here in the US as well but the things that I name GOB for banks, SAP for public trading companies, they do have requirements to have a security audit or a penetration test which is one of the services we provide. They are required legally to have one of those done depending on the regulation once a year, once a quarter, every time you make a significant change to the network or to the data structure you have to have things retested. There are regulations already in place that require organizations to have at least a yearly penetration test and security audit done.

Joe Dager: When I am looking at my IT structure and let’s say I am not a developer, I am a step removed. Is there something I should be looking out for, there should be someone obvious that I am being compromised?

Keatron Evans: You know what that used to be a lot easier to do that because systems used to be a lot more simple. We did simple things, and we only did a few things with our computers. Now we do everything with them. Browsers are smarter. The applications that we use are smarter and what that leads to is there are more bells and whistles. There are more moving parts. Now it’s harder to see that weird thing happening because there are always weird things happening with the increased functionality of what we do with computers.

What’s happening now is the attackers are evolving as well because one big part of hacking and penetration testing is something called the evasion and covering your tracks and it’s an entire art form around not setting off bells and whistles and not making where people can know what you are doing. In the classes that I teach; we spend an entire half a day just on teaching the students how to do that part. Okay, now you know how to break in, let’s look at how to break in without ever being noticed. We are doing classes for good guys; you can imagine bad guys or a really on the ball of that part of the attack factors as well.

Joe Dager: Should it be an external person to my company? This is really protected information. Should someone be trained internally or should I have a mixture with a quarterly review of some type or something?

Keatron Evans: You kind of need to have both. Basically having an internal person is ideal but the problem is most organizations that aren't over a certain size or generate enough revenue that really can't justify the cost of having an internal person whose full-time job is to do that. I mean once these people go out and get these certifications and they actually have the technical chops to do these security audits and to do these penetration tests, they are pretty high-salaried. If you are regular mom and pop shop with ten employees you likely can't even afford to have a person full time doing that so what happens is you are kind of forced to actually have someone external come in and do it once a year and pay him for that one time engagement vs. trying to pay a salary.

Now on the other side when we talk about regulations; if you are a big organization and you are regulated then not only are you required to have it done once a year, but you are required to have it done by the external third party. It's almost like even if you have internal pen testers you still are required to have an external one done. It's almost like you don't let a CPA audit their own books you know you have an external public CPA firm do it to maintain integrity.

If you are the organization and I hire you, and your job is to secure this organization, it's not likely that you are going to rate yourself poorly. I suck at this, and I didn't do a good job of securing the organization when audit time comes around; which is why they kind of regulate that you have a third party do it and not only that they regulate that every few years you rotate to new third party. You can't use the same third party over and over again because certainly if you do that too much that the third party becomes partly an organization extension. Like the Arthur Andersen-Enron thing that happened all the way back in 2001 where basically Arthur Anderson was no longer unbiased, they were kind of part of Enron. The relationships had developed so much.

You have to have it done externally if you are big enough to be under any type of regulations and it's a good idea to have it externally done if you are small just because trying to pay the salary of someone doing it internally is really not feasible and if you take a small company of like 50 people they might only have one or two IT guys anyway. Trying to give them the additional hat of now auditing and checking security that's not feasible because you have someone that's already stretched in and now you are adding up a whole other big responsibility, and you end up with not a good job.

Joe Dager: Well it makes sense too, because of the fact that it’s hard to see your own mistakes a lot of the times.

Keatron Evans: Yes, absolutely.

Joe Dager: Are there key things? Should my developer hire it done, when I use a subcontracted firm? How much should a CEO or CTO or someone be part of all that? What are a few of the questions that I should use to hire intelligently?

Keatron Evans: Well the main thing is to look for a resume. We live in a world of Google. We Google people first and then we talk to them, so we find out. So if it’s an organization or a person coming to you to offer service, you should be able to find information about them pretty readily on the internet as far as whether or not they’ve done good business. Also, it helps if you ask for previous pen test report. For example, if you are looking to have a penetration test done say hey! I would like to see a couple of sanitized penetration test reports that you’ve done for other organizations, and they should be able to provide that. That should show some of the maturity because that’s just one of the things people in the industry ask for.

They not only want to know you are technical and you are good at hacking but they want to know are you able to deliver me a report that’s going to allow me to make sound investments decisions and sound security decisions based on what that report says. Some of the best technical people out there has a really hard time relaying that information in a written form that people that aren’t technical can understand. I’ve been fortunate to have that I guess you could say gift because that’s one of the areas that I get a lot of traction and excel in business wise is being able to sit trenches and do the attack and demonstrate the attacks but explain what’s going on to someone that may not be technical at the same time so that when they look at ROI and what they need to invest in they have a clear picture. We call it enabling the decision makers to make the right security decisions.

Joe Dager: You are holding upcoming webinar okay, called *Find Out How The Most Secure Places In The World Get Hacked*. Tell me a little bit about that webinar. What are you going to cover in it and what are you going to do?

Keatron Evans: We are going to start that webinar off with a live attack. We are going to show you two attacks within a matter of like ten minutes just to let you see how quickly these hacks happen, how quickly they get onto your server, how quickly they get your data and then we will connect the dots and show you how if we look at the five big breaches in the last year one thing they all have in common is none of the attacks were complicated. They were pretty basics things, there were low hanging fruit that the attackers were able to get to and even if you take the biggest one which for example was Equifax; these are vulnerabilities that were discovered passively in security audits that were done much much earlier than the attack happened and they just kind of got ignored.

We think a big part of that goes back to what we were just talking about with the reporting properly and things like that where maybe someone did it and maybe the report got handed over, but it didn't do a good job of relaying the threat like what the actual threat was to the business decision makers. There was no action to be taken on that. I will go through and show the attack and then show you when we generate for example a report. The key things that you should look for in the report as a technical and as an executive that may not be technical. Here is what your report should look like number one and here is what you should be getting out of that report depending on what your job.

Just to kind of give people some free advice on this is what you should be looking for and also to paint a roadmap. A lot of technical people want to get into CyberSecrity, but they don't know how; I am going paint a roadmap on how you need to step yourself up if you want to really master these skills and bring that expertise into your organizations.

Joe Dager: What if I just want to be a hacker, are you going to help me out?

Keatron Evans: I can help you out too. We actually have classes that we train good guys up on that; the intelligence community, federal law enforcement, just the gatekeepers of fortune fifty companies, for example. A lot of those security guys that are responsible for security organizations, they come to me once a year or so to sit in a class to just to get the updates. What are the bad guys doing to us now? I will teach them some defensive mechanisms to keep those things from happening, and then we reset next year and start all over again because it's a rapidly changing threat landscape.

Joe Dager: You put effort into showing a hack take place during the webinar. Why do you think watching a hack is so important?

Keatron Evans: For one I think that when most people think about a hack, they think it of this complex thing. We say passively a hacker could do this or hackers can do or if you open this email, hackers could get stuff off in your computer. Well reading that in a paragraph and actually visually seeing it happen has two different shock factors to it. If you see it happen and if you see how easy it is, you see someone watching you type something, and you've seen your key, your letters, your word that you type into showing up on a screen somewhere else, that's quite chilling and quite eye-opening and awaking.

What happens is when you see it happen visibly it opens up a different muscle in your bran. You interpret the information differently, and it's a different shock factor when you see it versus when you are reading it in a paragraph somewhere. Reading articles about how these cyber-attacks happen is one thing. When someone shows it to you is another. The comment I hear most from executives is I didn't realize how easily it can be done. If you ask me the number one phrase I've heard from executives and others that have watched my demonstrations, the number one phrase is I had no idea that it was that easy.

What they realize very quickly is from how easy it is to do this that we should be checking for this. Why aren't we checking for this? I am going to go to my IT people and say are we checking for these things and that gets the conversation going. What I found is in any organizations if you can get the interest of the executives and the decision makers; when the security decisions are driven from the top down, you get a lot more action? If IT is a only one paranoid about security and only one doing something about security it's not going to have the same weight as a memo from the CEO saying you better not open that email that says you know you are going to get a million dollars if you send me $500 because you are exposing the whole organization to cyber-attacks. You are going to have a lot more attention paid to it.

I think everyone should watch these things at the executive levels because it empowers your organizations. The more educated the decision makers are for CyberSecurity, the more empowered the organization is to make more intelligent CyberSecurity decisions.

Joe Dager: What really intrigues me of the things you've said here is that it is actually preventable that you do have clues if you know what to look for and as you said the major hacks were in previous reports.

They were somewhat known. It's just the information wasn't transferred right. A lot of this is preventable with just a little bit of background and training? Is that fair to say?

Keatron Evans: That's fair to say. A lot of it is preventable and the ones that made the news are preventable but keep in mind there is an entire underbelly of cyber-attacks and breaches that never make to the news. Either they are classified or the organization; it's too embarrassing so they rather take the hit and not report it if they can get away with not reporting it. I don't want to make it sound like that you know everything can be prevented because there are really two classes of you getting attacked. One is you happen to be not doing a good job or paying attention to the basics things we are talking about and you just happen to get caught up in a sweep when they are looking for easy targets or the other side of that is if an advanced persistent threat targets you.

If you take one of these APT groups that are usually state-sponsored, that are usually funded by some government organizations and may target you, then there is not a lot that you can do to prevent that. If you look at a lot of the big breaches that have happened they were still compromised by very basics things. I don't want to make it sound like if you do these things, it's going to one hundred percent protect you. If you do these things, it's going to make it harder, much harder for these guys to get there. But if they target you and they have the funding, the resources, they are going to get in at some point, and there is really not a ton you can do about it.

There is a movement for in the industry at mature security organizations, in other words, companies that have a mature security program have kind of accept the fact that look, we are probably going to get breached at some point. We are going to get hacked so how can we continue the business? What's our process for business continuity? How do we increase our ability to detect that we've been compromised? There is a big movement in between protection and response where some of the resources are being devoted to that and not so much being spent on preventative, and what that leads to is a much better posture. If you really understand the attacks, then that puts you in the better positions to know when it happens because now you know what the attacks look like. You will see it happening a lot faster than someone that doesn't know what's happening until your data is for sale on the internet. Learning how to do the attacks and getting on the offensive empowers you to better detection and response decisions.

Now going forward in the future there is a lot of companies out there that are thinking things like machine learning and AI saying oh! We are back to prevention now. We can truly prevent because we've got artificial Intelligence and I would caution people of that. I actually have a conference coming up in Vegas in October of 2018. In that conference, I will be talking about the myths, the truth vs. the myths as related to how many of your CyberSecurity problems AI is actually going to solve. What amazes me is people seem to forget that if we are doing it, don't you think that bad guys are doing it as well. You are going to have two AI bots competing against each other and whenever we have that situation where the good guys and the bad guys are competing the bad guys have won historically. It's like we keep not learning lessons.

Every time we come out with the latest technology, we think that's going to solve all of our CyberSecurity problems. It turns out that later we find out the bad guys have already counted on us doing that and they've got countermeasures to get around that. That's where I see things going now, and that's some of the steps that we should be looking out for.

Joe Dager: Well I like that idea of the fact that you can… if you are watching, if you are not just all preventing is that there is a lot being put into as how you can minimize the damage and react to it properly is what you are saying is just as key as prevention.

Keatron Evans: Absolutely. One other point that I want to bring up related to that is I would say in about half of the engagements that I do about hack or penetration test; when I go and do a security audit even though we are not doing forensics, we are not doing instant response management about half of the times we find what we call indicators of compromise where the organizations are already breached. The bad guys are already inside, and they just didn't know it. Once we go there and start working with them and doing the engagement and transferring the knowledge, they start to see some of the things we are showing them, and they are like oh yeah! I think that happened six months ago, let's go take a look. We start pulling back the layers of that onion, and we find yeah! you've been compromised for a few years now. I mean they are constantly extracting data out.

Some of the penetration tests have turned into forensics and instant response gigs where they said all right! Stop the pen test. it's more important that you help us recover from this breach right now. So there is another contract signed you know that's different from the pen test that we were brought for in the first place.

Joe Dager: Your book for a good example Chained Exploits is a textbook still used by US government security agencies, and you also run certification courses. Tell me what it takes to get certified and what you teach in them. I think you've been doing certification courses for a while?

Keatron Evans: I have and to segway into that part of the reason I still do the courses is that I get an amazing amount of enjoyment out of sharing the information. Putting it out and watching people digest it and coming up with innovative ways to where people actually get it. That's kind of one of my passions, But yes! I've been doing certification classes for a long time. All of the top training organizations in the industry have used me for various types of classes. Our main class is Certified Ethical Hacker. We take someone with basic IT skills, and we bring them in and teach them the tools and techniques of hackers. They master those tools and techniques, and then we certify them at the end by having them take the official Certified Ethical Hacker exam, okay. It's a five days course, and on the fifth day, it's mostly testing. We do a half day of lecture and a half day of getting you prepared again for the exam. Then the second half of the last day you actually take the official exam, and you are certified when you leave on Friday.

We've just introduced a more advanced version of it called the Certified Ethical Hacker Practical. Not only you have to do the written exam, but you have to do about ten hour practical where you are attacking targets that we set up, and you have to break into those targets, get specific data off those targets and write a report. That certification is more advanced. It's definitely not entry level; people find it challenging because they actually have to not only prove that they have the knowledge from the written exam but they actually demonstrate it hands on. Those are the two biggest, the most popular classes that we run right now. Obviously, incident response is really popular, and computer forensics is still really popular as well. Those are the main core technical security classes that we run.

What we found when you were talking about how do you know if this is happening to you? One of the things we found Joe and we've got the data to reflect this is the number one way that we've been able to improve the IQ of the organization when it comes to whether or not they are attacked is taking their technical people and putting them in these ethical hacking classes. What happens is suddenly when they go back, and they are looking at their networks they are able to see signs, they are able to see indicators that they just couldn't see before because they hadn't been exposed what these attacks look like.

Joe Dager: Are you putting a class on shortly? Do you run these often, or when is your next class?

Keatron Evans: The next one that I am running…. There is one on September 10th in Birmingham, Alabama. It will be a pretty good one. We have some good people signed up, and I wanted to kind of point out one of the values that come out of these classes too is networking? You have an IT security guy from this bank, and then you have an IT security guy from another bank, and they start talking to each other. They share threats, and they learn from each other just as much as they learn from me sometimes on certain topics. I've even seen great connections like people end up with jobs. There might be a person that's maybe he is working as a Geek Squad, a technician at Best Buy or something like that. They want to get into CyberSecurity. They come and takes the class while also in the class is a Chief Information Security Officer for a Fortune 500 organization that's looking to hire people. If this guy is really good in the class, then that person ends up with a job offer all of a sudden.

The learning is a big part of it, but there are other peripherals things that people get out of these classes; the networking, getting jobs and even getting employees. For myself, my practice I've got some of my best employees from classes that I've taught, and I've been able to pull people out of those classes that are unemployed. Obviously, we can't hire people that already have jobs because that would be a violation of integrity for your company to pay me to teach your employee, and then I steal them from you. In our training, we have a contract that says that we won't do that. We will also prevent your employees from getting hired on with other people. If you need a job, this is one place to come. In this class, you can probably get hooked up because there are a lot of people able to make hiring decisions in these classes.

Joe Dager: Well it's a fascinating subject, I think fascinating space to be in right now. Is there anything that you would like to add to this conversation that maybe I didn't ask?

Keatron Evans: We do quite a bit of public outreach and evangelism. On our website kmcybersecurity.com, I've got a very popular article that I wrote just a few months ago, and the article was titled, *How to get into Technical Cyber Security. W*hat your steps should be to get into it. It's been a widely received article. It's been shared on LinkedIn and places like that, thousands of times. We are going to start now doing more of laying out a roadmap doing outreach to show people… we want to become the go-to-bridge, for people to get into CyberSecurity. Whether you have money or not, whether you have taken classes or not; even if you have taken a class somewhere else or taken it from another provider. We kind of want to be a bridge to show you look, go do these things first before you sign up for any class. This way everybody ends up with a successful experience taking classes.

Joe Dager: What's the level of IT knowledge that I need to take the class, to get certified?

Keatron Evans: I think you have to have what we call power user level skill or better. For example, if you are listening if I were to say, tell me one of those IP addresses, can you do that? If you can do that,, then you are probably a power user. If I were to say Ping Google.com and see if you are getting a response, if you know what that means then you can set down your computer and execute that then you probably at that power user level. That's kind of the level check for us to see if the person has the right skills or not. If you've never seen one of those command lines before then maybe you are not, maybe there is some remediation or some things you need to kind of beef up on before you take a class like that and again that's part of what we are doing in outreaches. We are creating that hey can you do these ten things. If so you are ready, if not go look at these few videos and learn how to do these before you sign up for a class.

Joe Dager: I would like to thank you very much. What's the best way for someone to contact you?

Keatron Evans: They can reach me on the website, or they can also just reach me at KEvans@kevanscybersecurity.com.

Joe Dager: I would like to thank you very much Keatron. I find this field fascinating. This podcast will be available on the Business901 iTunes store and the Business901 website. So I want to thank all the listeners for listening.