A Conversation With the “Original Internet Godfather”

During the closing session of the 32nd Annual ACFE Global Fraud Conference, John Gill, vice president of education at the ACFE, spoke with convicted fraudster* Brett Johnson, who shared stories from his life as a cybercriminal. After being placed on the United States Most Wanted List, captured and convicted of 39 felonies, he escaped prison. Captured again, Johnson served his time and accepted responsibility.

Transcript

**John Gill:** You have an interesting moniker that I think the U.S. Secret Service gave you. What is that and how did you get that?

**Brett Johnson:** Wow, that's a question. The United States Secret Service, they called me the “Original Internet Godfather.” How did I get the title? That's the question, right?

Thirty-nine felonies.

I was placed on the United States most wanted list. I escaped from prison. The big thing, as if that's not big enough, the big thing is that I built the first organized cybercrime community. It was called ShadowCrew. It was a precursor to today's darknet markets. It laid the foundation for the way modern financial cybercrime markets operate today. That's Brett. Those 39 felonies had to do with refining a lot of the different types of online financial crimes that we see today from account takeovers, credit card fraud, phishing schemes, tax return identity theft … basically everything is still going on today or the types of crimes that you see being innovated today begins back with ShadowCrew and that group that we formed.

**John:** Do you have any insights? Can you help us, what is the lure of the cybercrime? Is it the anonymity of it or do you think it was a lot of, “Well, they can afford it, these are companies.” Why did it have such a hold on you?

**Brett:** It is an addiction of sorts. Not even of sorts, it is an addiction, but committing online crime, the real difference, actually, there's a few real differences. We'll talk about this, but one of the big differences is that you never have to face your victim. Typically, in a crime, if you're victimizing someone, there's some sort of contact with that victim. Even if it's by phone, you're still in contact with that victim, you get to hear the victim's voice, you get to hear the pain and the suffering in that victim's voice. Most crime though is face-to-face, a lot of it is, so you have to face your victim. When you're online, you don't have to do that.

Not only that, but you can compartmentalize, and I did. You can compartmentalize your online life from what you've considered your real life. You can say, "Online, yeah, I do all this stuff online, but in the real world, in my real life, I'm a good guy." That's that buffering, that compartmentalization that a lot of criminals do over and over again. Even with me, I did the exact same thing. I justified it. I was like, "I did it for my family, for my wife, for my stripper girlfriend." There was a lot of justification, a lot of compartmentalization, and there's also a hierarchy that develops the more you commit crime.

You get to the point where you're saying, "Well, I don't hurt people. I just steal from governments and businesses that can afford it," which is a complete lie. I mean, with the number of victims, you always
start out, and I'm no different, I started out victimizing people, pretty mom and pop shops. Finally got to the point where you're hitting governments, and then you're hurting everybody because everybody pays at the end of the day.

It's the compartmentalization, it's the justification, it's much easier, it's not having to face your victim.

You also need to realize that the way cybercrime operates, there are three basic necessities to committing successful cybercrime. Those three necessities are gathering data, committing crime and then cashing out. When I talk about gathering data, that's still criminal activity, but not from the criminal side, not from the criminal viewpoint of things. That's just getting all the information that you need and the tools that you need to commit the crime. It's stealing PII, it's acquiring SOCKS5 proxies or spoofed numbers, anything else like that, remote desktops, VM boxes, whatever the tools you need, plus the bank account logins, the stolen socials, anything else you need to commit account takeover, set up new accounts, credit card fraud, what have you.

What you see with those three necessities over and over again — gathering data, committing crime, cashing out — what you see in those three necessities is that one single criminal is not good in all three. He's good in one thing, sometimes two, and rarely, I mean, rarely do you ever find someone that can effectively do all three things. The way that cybercrime operates is you have these large structures, whether they be marketplaces or forums or telegram groups, or what have you. Those structures primarily exist so that that one specific criminal who's good at one thing can network with other criminals who are good in things where he's not.

Take me as an example, I was always very good at committing the crimes and then laundering the money. All right, gathering data, no. Now I can do it, but I suck at it. Why would I spend my time doing that when someone is much more effective at that particular thing and that's what you see all the time. You see the marketplaces that are set up that sell illegal goods, whether it be drugs, whether it be PII, bank account, logins, credit card information, what have you. Those people know how to gather the data.

Typically, they don't know how to commit the crime. They couldn't use stolen credit card details, if they've tried to they. They certainly couldn't cash it out, but they can gather it and they know how to sell it. So those are the information gatherers. Then you've got the people who commit the crimes. Then finally, you've got the people who cash out.

We've had a lot of problems recently with stimulus fraud, specifically unemployment fraud. That's one of these case studies on the way cybercrime operates.

**John:** We'll stay with a larger issue, one thing I do think is interesting is the idea of organization because I think, at least in my generation, a lot of us, when you think of hackers, think of cybercrime, you think of somebody sitting in their mother's basement on the computer, but it's grown from that. Now, this is an organized industry. It's organized crime. When we talked two years ago, we talked about ransomware. Now that's made a big comeback recently. People are obviously extremely concerned about this, and they should be.

This has had a lot of economic impacts in our country and elsewhere around the world. I know you at least are keeping tabs on things like this. Can you give us some advice on how we can combat this, what we should be alert for or what should we know?

**Brett:** Sure. So let's talk about ransomware for a second. We had Colonial Pipeline hit. They pay the ransom. We had JBS hit. They pay the ransom. We had the PGA hit a couple of years ago. They pay the ransom. When you pay ransom, what does that do? That tells the criminal, "Hey, this works." Not only does it work, but it's extremely profitable. First of all, how is ransomware deployed? Typically, it's deployed by some sort of social engineering techniques, some sort phishing scheme, spearphishing scheme, maybe dropping a thumb drive in a parking lot and see who plug it in because they will. It's looking at cybersecurity issues.
If you've got—and here's a stat for you, 41% of every single router on the planet has a default password. Think about that for a second, 41% of every single router. I don't care if it's a bank router, they have the default password. It's very easy to get access, very easy to get access. I was on a panel a couple of weeks ago that was talking about ransomware, and one of the ideas that was put forth was when it comes right down to it if your business is hit with ransomware, it's a business decision on whether you pay the ransom.

No, no, I'm going to say if you if it gets to the point where you're saying it's a business decision on where you pay ransom, the problem is that you did not prepare properly as far as your security goes.

Here's the thing, this is a fine line to walk. It is never the victim's fault that crime happens. It's always the criminal's fault, always. It was not Colonial Pipeline's fault that ransomware was deployed on their system. It's not JBS's not. It's not the PGA's fault. It's always the criminal's fault that crime happens, but if you live in a neighborhood where you know crime is huge, you probably want to lock your doors when you leave the house. That tends to be the problem with cybersecurity. More often than not, we see that companies really don't worry about cybersecurity until they've been hit with an attack. They don't want to put the money for it.

Typically, you have an IT department, and the IT department will come and say, "Hey, we need these tools." Management will say, "Not right now." It's never a question of if you're going to be hit. It's a question of when you're going to be hit. Usually, it's a question of, well, it's not your first time, is it? You just didn't know about it before.

We have to get to the point where we take a proactive response to security. Everybody, I don't care if it's an organization or an individual, you have a place in the cybercrime spectrum. Everybody. If you have a business or an organization that makes money, a criminal can and will make money off that same business or organization. Understand your place on the cybercrime spectrum. The way that I will victimize you differs on who you are and what you do. For example, if you're an individual, if you are the CEO of a company or you work payroll, the way that I will victimize you differs from if you've worked food service for 20 years. I'll still victimize you. If you're CEO or payroll, I may try to implement some sort of business email compromise scheme. If you've worked food service, I may set up new accounts in your name. I may try to commit HELOC loan or student loan fraud in your name, may do any number of things, I'll still victimize you.

Same thing for a company. Does your company have data that I can breach the company, steal the data, resell in the black market, or is the data specific to the company? That will determine whether I try to steal the data and resell, or whether I try to deploy ransomware on the system. Understand your place in the cybercrime spectrum.

Also understand that most of these crimes are effective because of social engineering. What social engineering basically means is compromising the human. Tools tend to be very good, but you're compromising the human. You're sending those phishing emails, you're relying on management not to trust their IT department. We see this time and again. That's one of the things about organized cybercrime is the intel, the data among criminals is real time.

Criminals know if a company has changed fraud teams, if they've changed tools, if they've started using a new fraud tool, stop using an old one, that they've implemented some new security. If security is lacking, then they share that within their entire network, and these networks are millions of members large. The data is real time, the intel is real time, it's always up to date, and it's always about compromising the human. As such, we need to constantly be training the humans, but we also need to rely and trust the tools. The tech tends to be very good.

If you're not implementing the proper tools, if you're waiting until you're hit, it's wasted. I'm a firm believer, the French recently, the French insurers stopped paying ransomware. I think that's one of the best things that could possibly happen, because at the end of the day, companies are not … unless they're forced to implement proper cybersecurity, we're going to continue to see these types of attacks.
We're going to continue to see that idea, “Well, we're okay right now, we've not been attacked.” Cybersecurity should be mandatory. Insurance companies need to stop paying ransomware. That will help force companies to prepare effectively on their security side, instead of…

To any company out there, I would say, instead of stockpiling Bitcoin, use that money to implement proper cybersecurity. That will be much more effective at the end of the day.

**John:** When you say proper cybersecurity, when we talked before, so first of all, I do agree. It seemed to be previously, when we talked to companies like, “Well, how do you feel about how vulnerable you are?”

“Oh, well no, no, we have a firewall, and we have antivirus software, so we're good to go.”

As you've said, we've discovered that's not enough. One of the things I know that you've been a big proponent of, and we have too, is training employees. I've seen surveys that say, as you mentioned, that is often the primary way that they're getting into the organization is through some … they clicked on the wrong email link, or they download an attachment, it's through the human being.

That's one of the first things that the companies can do is train their employees. Then when we talked before, you mentioned back up your data. If you are hit with ransomware and you have everything properly backed up, then you don't have to pay the ransom.

**Brett:** Right, it's all preparation. With training, I'm a firm believer in proper training and persistent training. Studies have shown that as long as training is ongoing, that employees tend to be extremely good. They tend to be vigilant. They tend to be aware of problems and the techniques that criminals are using to hit companies, but when training stops, at that point, they're right there at the top, and when training stops, guess what, the awareness levels, everything else starts to go down. Training needs to be persistent. It doesn't need to be some 30-minute video that you watch every six months, it needs to be persistent and consistent.

Backups, backups are extremely important. I can't stress that enough, and they need to be separate from the system as well.

There has been three years ago before I talked to you last time. I get a call one day from a medical goods supplier out of Knoxville, Tennessee. They had been hit with ransomware. My first question was, “Do you have backups?” He's like, "Oh, yes, we got backups." Then he pauses and he's like, "They're locked down too." That's the problem. Backups are good, but you have to make sure that they're deployed properly. It boils down to doing things properly.

It's more than just backups and training. It's making sure that you've got all the tools in place that you need. Those are some of the most important, but a criminal, it's more than social engineering, 90% of it's social engineering, but a criminal has a variety of tools that he uses to attack you. You need a variety of tools to defend yourself as well.

The thing about it is they're not horribly complicated tools to make sure you're not that lowest hanging fruit on the tree. It's password managers or if you're a company, if you don't want to use password managers, you can get the hardware that plugs in that secures you so that phishing stops completely, the hardware keys. You get that. It’s the training. It's making sure that you're looking at all the data that comes in. These days, if you look at security and companies, the way that things have been is everything has been siloed. Well, criminals are used to that. Criminals tend to take one silo and defraud that specific silo based on its own merits. Then once they gain access to that one silo of security, it allows them access to these other silos, whether that be a security operation, or whether it be, if you're trying to commit some identity fraud or something like that, you defraud one where it doesn't look like it's fraud within that system, that system doesn't suspect that type of fraud, but it allows you access to these other systems.
Then you use them all together to commit whatever you're trying to do. Kind of complicated, but really effective. We, as the good guys have got to the point now, I see more and more companies that are starting to put additional tools. You've got a lot of identity protection companies now, identity verification companies that are starting to look at biometrics on top of that, that are starting to acquire data services on top of it.

It's the idea that even security companies now are starting to understand that one tool doesn't solve everything. It takes a variety of tools. The more we get to that point of understanding, the more effective I think security is going to be in. As I said before, it has to be proactive. You have to be proactive with this stuff.

**John:** Well, that's the good news, that there are always prevent it. The bad news though is, from what you explained, they don't really have a conscience when it comes to cyberfraud. That's their business. If you think they're going to take mercy on you, if you beg and plead, is just not going to happen at all.

**Brett:** Well, think about JBS. JBS, right now we've lost 20% of food supply, the meat supply. The people who've launched that attack, I think it's REvil that did, that RE-evil. The people who watch this, they know that they have hurt the entire planet as far as meat supply goes. What does that tell them? That tells them, "Hey, this company's sweating. They can afford it. I'll bet they pay."

"No, we're not going to negotiate."

A lot of the times with ransomware, you can negotiate with these people. If they want $2 million, you can sometimes negotiate them down to $200,000. You get something like that, no, we're not going to negotiate. The ransom is this, you're going to pay it or not, I bet you will. I bet you will.

**Interviewer:** They do.

**Brett:** They do. The way you don't pay, is you prepare properly to begin with. You don't take the idea that, well, we might not be hit. No, it's always when. When are we going to be hit? You prepare properly. You trust your IT team. You hired these guys for a purpose. Trust them because they won't steer you right wrong.

**John:** Good. Well, Brett, we're out of time. That's a lot of good advice. Thank you for sharing your story. I'm glad that you are trying to help prevent the problem and not one of the causes now. That's a good thing. You have your own company that you use to do speeches and training. Is it Angler Phish?


**Interviewer:** Thank you for sharing your story. It's interesting, and it changes constantly. The only thing we can do is just keep up with it, and like you said, implement the tools and be prepared.