RACE TRACK INDUSTRY PROGRAM

40th ANNUAL
GLOBAL SYMPOSIUM ON RACING & GAMING

WEDNESDAY, DECEMBER 11, 2013

Cyber Security (or Lack Thereof)

MODERATOR:
Vin Narayanan, Editor-in-Chief, Casino City

SPEAKERS:
Gus Fritschie, SetNet International
Hai Ng, Partner, Neomancer LLC

Ms. Liz Bracken: Thank you for joining us for this panel. The Vin and Hai show will continue.

We had 'em this morning, and if you were at that panel they were very informative and really good to listen to.

This panel is gonna be a little bit of a different topic, and a fairly serious one, cyber security or lack thereof.

This panel is sponsored by Sportech Racing and Digital, who is also our Diamond sponsor for the conference, and we would also like to thank Del Mar Thoroughbred Club for our beverage break.

I will turn it back over to Vin and get going.

Mr. Vin Narayanan: Thank you. Much appreciate it. Thank you, everyone, for sitting in on this session.

Cyber security can be dry, but we'll try to keep it a little lively here and keep it moving.

One of the things we did when we were asked to do this cyber security panel is we kept an eye out in the news and sort of out there for things that were happening from a cyber security standpoint as the conference was approaching, and were like there's something that's gonna happen that we're gonna be able to talk about.

As luck would have it, there sure was.

We have two incidents just to give you an idea as to what the threats from a cyber security standpoint are before we get into the overall discussion.

A couple weeks ago we had something called the Pony, and we couldn't believe our luck when there was an attack from a Pony out there.

The Pony was a piece of malware that was put into people's web browsers, basically, and — well, it was put onto people's computers, but it stole passwords stored on users' browsers.

Those stolen passwords ended up exposing over two million user passwords. 57 percent of them were Facebook passwords.

You had Yahoo, Google, Twitter accounts, LinkedIn, all of these passwords exposed.

If you work in — If you're dealing with any sort of web service that has a logon and a password, this is the type of thing that you have to be worried about, malware coming in and stealing passwords.

A lot of these passwords, it was just they happened to be weak passwords that happened to be stolen as well.

Then in the last week of November the *Racing Post* was hacked out of Great Britain, and the *Racing Post* is a big site out there.

Fortunately there was no credit card information stolen, but you got real names, mailing addresses, logins, and passwords stolen.

The *Racing Post* came out and admitted — they didn't say how it happened. They said it was a very aggressive attack on their system, though, that stole all the logons and passwords.

This is real, folks. Cyber security is real, and it's a serious issue that all of us have to deal with.

When you're dealing with money and the handling of money, it just makes it that much more real.

Joining me to talk about this today is Hai Ng, who is here on the panel. He's the mayor of this conference on Foursquare, and he is also a security expert, and Gus Fritschie, who works for — hold on. I had this.

Mr. Gus Fritschie: You don't have it memorized?

Mr. Vin Narayanan: SeNet International Gaming.

Mr. Gus Fritschie: Thank you.

Mr. Vin Narayanan: Yes. I have to take notes because I'm losing my hair, I'm getting gray, and I just forget stuff.

Mr. Gus Fritschie: We all are.

Mr. Vin Narayanan: The real reason they put this panel together is we have the best hair of the group.

We're gonna talk about that.

We're gonna start with Gus here. Gus has a great presentation for us. It's gonna walk through some of the security threats that are facing us right now, but before Gus gets up here, just wanna poll the audience here.

How many people have ever worked in IT?

All right.

Mr. Hai Ng: Two, three, four.

Mr. Vin Narayanan: Yeah, it's two or there.

How many people think they have really good security for their web services that they're offering?

Nobody.

How many of you are offering web services?

All right.

We've got a handful.

Go ahead.

Gus is gonna get up and talk about it a little bit.

We like to do this poll so it gives an idea who we're talking to, but also gives an idea of what we wanna cover as we're rolling around.

Gus, I will hand it over to you.

Mr. Gus Fritschie: Great.

Thank you.

I have to go — sorry. Yeah, thank you for that introduction, Vin. I put together a short presentation.

Probably should just take about ten minutes, and then we're gonna move more into the panel discussion that Vin led in the social gaming discussion.

We'll go over and bounce forth a variety of different topics, but just wanted to put together this and highlight some of the more interesting issues that I see in play.

Just first who I am.

As Vin noted, I work for SeNet International.

We focus on online gaming and also the gaming security sector, and of course the horse racing industry comes into play, and we provide a variety of different security services centering around that.

Who am I? I'm the CTO of that organization.

I do think I am a subject matter expert when it comes to gaming and i-gaming security.

At least I'm one of the only ones out there that's actively researching and talking about it and presenting at different conferences, both in the security and in the gaming sectors.

Mr. Vin Narayanan: Your daughter is pretty sharp, too.

Mr. Gus Fritschie: Thank you. Thank you.

Yes, she's learning how to play poker there.

She's much older.

That's an old picture.

I also written many articles, so if you're interested in that, they're out there, and I think we may discuss one of those more recent ones that I published recently.

Also, if you wanna follow me on Twitter, I primarily tweet about gaming and other security related issues.

Why this talk? I was very happy to be asked to be on this panel discussion because I've been attending a lot of different gaming conferences over the past two years, and very rarely is there a specific panel discussion on security.

Of course, I think it's a very important topic and I hope most of you do. I see if you're in this room attending, you probably agree. My opinion, that the future

success of the horse racing industry is gonna be tied toward the internet and i-gaming.

Even if it's not specifically, there is your internal security controls. They still need to be secure.

Even if you're on a closed loop network, you still have internal security concerns, and Hai will talk a little bit about that when we get to social engineering and how your users could be attacked.

While I think the racing industry has had a head start compared to, say, the casino i-gaming sector due to the carve-out they had in UIGA legalizing it, or at least not specifically saying it was illegal, we need to learn from those past mistakes that have been made in these other sectors, both gaming and perhaps other industries as well.

Often security is seen as a cost.

You don't obviously see an ROI right away on it, but unfortunately, just like the analogy of a leaky basement, you don't think about it until it's a problem, and often then it's too late and you have to pay a lot more money to get it fixed, where it would be much cheaper to fix it earlier on.

How is online racing different than this?

Of course, now we all know where I bank at, but Wells Fargo, I know several people there.

Very secure site.

Is there any difference between banking and i-gaming, horse racing online?

In my opinion, there really isn't much difference.

At one point in time, I had a lot more money in my poker account than I had in my bank account.

Maybe that was naïve of me.

Mr. Vin Narayanan: I hope you got it out.

Mr. Gus Fritschie: Some of it, Vin.

Mr. Vin Narayanan:

[Laughter]

Mr. Gus Fritschie: You need the same type of controls in online racing i-gaming that you need in other sectors, like financial sectors. Maybe you don't need the most stringent controls, but you need to have some level of security there.

There's a lot of different areas that we could talk about, and you see some of 'em up there. Application, system, database, mobile.

Obviously we don't have time to talk about all those, but these are all factors that do come into play.

What I think is very important, and I think the gentleman in the earlier presentation talking about the physical security and disaster recovery and risk, and you need to determine what your risks are, and he was approaching it more from a physical threat standpoint from terrorism or et cetera.

The same point can be made toward information security, too.

You're never gonna have a hundred percent security. You would have to unplug from the internet and not do business that way.

It's all about understanding what your risks are, and then being able to manage them. I think earlier on — and we've seen in Vin and Hai's presentation earlier about social gaming and some other ones about new ideas, new technologies that need to come into the racing sector, if it's social gaming, if it's mobile, if it's i-gaming.

There's technologies that we haven't even thought of yet. They all pose security risk and us as security professionals, we can't go and tell you, no, you can't do that, because then we're not enabling your business, but we wanna be able to make sure you can do it in a secure manner, and that's key.

You can do this in a secure manner. It may cost a little bit more. It may take a little bit more time, but you wanna go about and know what those risks are so you can make those business decisions.

I think a lot of people would say is compliance the answer to this, and I think Vin will have a little discussion about that later on in the panel.

These are just, of course, obviously various compliance standards, and, of course, there's regulatory standards in the gaming sector as well as in the racing standard, but for the most part they're pretty weak.

In my opinion, compliance does not equal security, but it's a starting point. We'll touch on that more in our discussion on the panel.

What is the solution?

It's a comprehensive, enterprise-wide solution, way too long for this brief presentation, but in my opinion there's two key ways that organizations are getting compromised today.

One is through attacks via applications, so if you're making web applications available to your customers to bet, interact with, both web-based and mobile, the handhelds.

Then, of course, social engineering attacks, which Hai is going to touch on.

Most organizations have solved some of the other types of attacks as far as protecting your perimeter security from the internet, but in order to do business you need to have web ports open, and that's what attackers are looking at. The rest of this presentation is gonna look closer at that first method, application attacks.

I'm gonna try to keep this not too technical cuz I realize that we have a mixed audience in here, but OWASP is an organization that has a lot of great advice on web application security.

I just wanna tie this back to two of the points that — or one of the points that Vin brought up with the *Racing Post* attack and how that database ended up being hacked, and a lot of user names, personal information was extracted from it.

From what I could tell, from the research I did, it was via a SQL injection attack.

You can see there, that's A1 as far as one of the top application vulnerabilities.

It goes to show you that you're making most of these applications interface with some type of back-end database, and if the code is not designed securely, if a database is not secure, it is vulnerable.

Just to touch on another one of these and tie it back to one of the previous discussions, broken authentication and session management.

A gentleman was up here from Derby Wars talking about it, and this applies to daily fantasy sports as well, but think about it.

Part of that is you go ahead, you set your lineup, you pick what horses you want, and you're competing against someone else, but what if your competitors knew who you were picking ahead of time?

They would have an advantage of knowing if they wanted to bet against you or not. Depending on how well these applications handle authentication, session management, et cetera, there could be vulnerability.

These are all great ideas to look at. I'm not gonna spend too much time talking about it here, but OWASP, for those of you who deal with application security, is a great guide.

What's the answer?

I'll tell you.

It needs to be built in in the beginning.

As these different applications are being designed and developed, you need to build security into the system development lifecycle. If you wait 'til the end, it's too late.

It's gonna be more expensive to go back and fix those vulnerabilities. If you're designing your own applications in-house, you want to make sure that you're building security in.

If you're procuring them from some type of service provider who's designing — who already has the platform available, you want to be asking questions as far as how did they vet the security?

Did they have independent assessments done?

Have they had code reviews done? Et cetera, et cetera.

It's boring to sit here and look at a bunch of just text.

We all want examples, and when Vin asked me to be on this panel, I have to admit, I'm not — I didn't know too much about the racing industry, what was available online.

I used to bet on Bodog, but obviously I don't anymore since they pulled out of the U.S.

I really hadn't looked at any other alternatives for betting horses online, so I decided to take a quick look at some of the sites that were available.

I did find some vulnerabilities, in my opinion that I just wanted to illustrate some of the points and tie it back, and then we'll jump into the panel discussion.

First, I wanna say that I have redacted some of the slides that you'll see to remove the name of the company on those I think are serious or more serious.

Several I've left the website on there because, in my opinion, they're a low-level vulnerability.

Some even say they're informational, but they still illustrate the point that vulnerabilities exist out there.

Also I wanna note that all this was done from a passive perspective.

I only watched the traffic go back and forth between my web client and the web server.

I didn't actually attack any web servers as I did not have permission to do so.

That said, let's look at some of these vulnerabilities.

Session token in URL.

I realize that the slides may be difficult for those of you to see in the back. It's difficult for me to see from where I'm sitting, but in the rectangle box there is basically a session ID that's being passed in the URL.

This ties your unique session to the particular client that you are.

Why is this bad?

Well, because if you're passing things in the URL, it can be intercepted.

It can be sniffed.

It's gonna be cached on your client. It's better to be done as a — stored as a cookie, per se.

This is just showing little things that, in my opinion, should not be present in an application that's accepting bets and real money online.

Once again, this is low-level vulnerability, session token in URL.

I'd be more than happy to talk about any of these later afterwards, for those of you who wanna talk tech and get more detail.

Account number enumeration.

Some of the sites did a very good job if you typed in the wrong, an invalid account number.

It comes back and says, "You either have an invalid account number or a wrong password," so it doesn't tell you which it is, but this particular site, if you typed in the account number, it basically says it's not defined, so you know that account number doesn't exist.

Then you can go until you find one that does exist and then you could brute force that password.

A simple fix.

Once again, a low-level vulnerability, but something that really probably shouldn't be present in a production system.

This one, in my opinion, was a little bit more serious.

This is one of the sites, and I was monitoring the communication, as I said, back and forth from my web browser to the back-end web server, and I noticed that there was a request — and this will be better seen here.

This particular request, and I've edited out the information that shows the specific site, but what most of you see when you communicate on the web, you just — you're clicking the web browser.

You don't see what's going on in the back end, but there's a lot of raw web http requests that are going back and forth, and if you know what you're doing, which is — this is trivial — you can intercept those requests, modify 'em, view 'em.

Here you can see I was checking previous play history,

I think, in my account, and I noticed a back-end web request.

You can see there's actually a username.

That's not my username.

That's not my password.

That's not my IP address.

That's a communication going to a back-end web server, and for whatever reason they've coded it incorrectly and they're passing that as a parameter in the JSON query. Not really the best security practice.

What is this?

Any idea?

Audience Member: Password.

Mr. Gus Fritschie: Yes, you're right.

Password.

Mr. Vin Narayanan: Hopefully it's not yours.

Mr. Gus Fritschie: Hopefully it's not yours, but

[Laughter]

— but this is what Vin noted in that Pony malware attack.

Someone did some analysis, and from all the passwords captured, this was the most common password, 123456.

Once again, let's take this with a grain of salt because, from what I've read, most of these systems that were compromised via this malware were like home users' computers, et cetera, et cetera, running Windows systems.

Probably not very sophisticated users, but that might be many of your customers.

It all relates back to weak password policies, and here are just two from two different sites.

You can see it.

It's just six to ten characters.

This other one, actually, in smaller print, doesn't allow symbols or special characters.

Once again, just something that you wanna enforce strong passwords. It helps protect your site and your users.

Passwords stored in clear text.

Here I used on a site, which I've redacted the information, the forgot password function, and you can see it says, "Dear Gus, your recently requested password for my"— for the site account. "Your username is" — I redacted my username cuz I don't want you guys to hack my account —" and your password is password1."

It actually gave me back what my real password was, and if you know anything about encryption in databases, there's no way it can really give me back the clear text password if it is really being encrypted, hashed, and salted like it really should be.

Most likely the site is storing your passwords in clear text in the database.

Once again, not the best idea.

Cross-site scripting. This is another one of OWASP top ten vulnerabilities.

It's a JavaScript attack against the client, and here you can see in the GET request — you probably don't understand a lot of this if you're not a programmer, but it's the script alert is executing JavaScript on the client to do a pop-up of its XSS.

I mean you can see in the site XSS is popped up. This is just a proof of concept. You could steal cookies. You could do more malicious activity, but, once again, this is on a production horse racing site that is collecting real money for bets.

I ran through that very fast because I wanted to make sure we had enough time to have the panel discussion, but this was just introduction of some of the security issues that I discovered in, really, less than an hour, just casually looking.

Think what a dedicated attacker who really wanted to target your site could do if they had the reason.

During the rest of this panel discussion, we'll dive deeper into a couple of these issues.

I know Vin has a lot of interesting topics that we wanna talk about. We know a lot of security questions could be sensitive, so if you don't feel comfortable asking them in a group setting, feel free to ping us afterwards.

With that said, Vin, I'll turn it back over to you.

Mr. Vin Narayanan: Thanks, Gus. I appreciate it.

Now you guys know why I like to hang out with Gus. He keeps things honest and secure, and it's good.

If you've ever been to a hacker conference or seen a hacker conference or anything like that, it's enough to scare you straight.

You go there and you walk out and say, all right, we've got to fix all this stuff because anything can happen.

I mean some hacker conferences, you have a secure Wi-Fi and an open Wi-Fi, and if you dare to use the open Wi-Fi, all that stuff's intercepted and put on a video board somewhere just to prove a point.

I think, for me, one of the big takeaways, Gus, before I get to Hai — and I think Hai would echo this — is the importance of building security in early.

Retrofitting for security is really, really expensive, and you don't wanna learn an expensive lesson.

You might as well take care of this stuff in advance, cuz otherwise you could be in a lot of trouble.

Mr. Gus Fritschie: No, absolutely, and we see this in other industries.

No one has to tell you about healthcare.gov, and there have been a ton of vulnerabilities that were discovered in that site since they went live in a rushed approach.

Now they're have to scramble and spend a lot more money to fix those issues, and obviously that's a much bigger profile target than any of you guys would ever be, but yeah, it's definitely a very good point.

You need to build it in early if you can, and if you can't build it in early, you still need to get it looked at later on to know what your risks are.

Mr. Hai Ng: It's the same as if you were in construction.

If you plan for security when you're planning your job, it's a lot easier to build it while you're building everything else than to build everything else first and then figure out where you're gonna put the locks and all that, because you may have to tear certain things down in order to do it or you may have to compromise.

Mr. Vin Narayanan: Now, one topic that Gus deliberately skipped was distributed denial of services.

It's something that I'm gonna talk with Hai about here.

For those of you that don't know what it is, it's basically — let's just say you have a website. You get a network of computers that just are pinging and pinging and pinging your website to the point that the website can't load anymore.

It's trying to answer all of these requests for data information. It just gets overloaded.

Right now in Europe, in the online gaming scene right there, you get tons of distributed denial of service attacks in online casinos and online sports books and that sort of thing.

What they do is they keep hitting your service until you're shut down, and then they call you up and they say, "For $100,000 we'll stop doing this," and some folks pay the ransom, and —

Mr. Hai Ng: Well, some of them are actually nicer. They will send you the ransom note before they shut you down.

Mr. Vin Narayanan: Yes, and some of 'em are nice and send the ransom note.

This is a very real threat.

I mean consider this.

You're approaching Derby day, biggest day of the year, and you've got your betting systems ready to go, and then all of a sudden you can't pull up the website. You can't pull up the betting system to server. You can't pull anything net up because someone's decided to attack you on Derby day.

Are you ready to handle something like that? That's a really serious question, and so this is where I'm gonna start with Hai, is I mean — first, did I accurately describe DDoS?

Mr. Hai Ng: Well, yeah. That's essentially what it is.

We call it DDoS for short, or DDoS, distributed denial-of-service attack.

A very practical, real-life example of it actually happened a few years ago to Best Buy, and this is actually a physical version of a DDoS rather than a virtual.

What a group of people did was they did a flash mob and, if you know what — for those of you who don't know what a flash mob is, is they sent out a bunch of texts to people who were waiting to do it with instructions where to meet.

For that particular Best Buy it was show up at that Best Buy with a blue shirt and khaki pants, which if you've been to a Best Buy, that's what the sales associates wear.

They had about 30 to 40 people show up and they all went in the stores and started mingling.

What it created was customers thought they were working, and they would start asking them for questions and they would say, "No, we don't work here."

The customers couldn't figure out who was working there and who wasn't.

They didn't break any laws because they didn't pretend to be associates, but they prevented business from carrying on.

Another example would be a flash mob that would send a thousand customers into your track, potentially, standing in front of your cashiers.

If your legitimate customers can't get to the cashiers, you can't do business and they've, in essence, shut you down. That's what happens in DDoS in the virtual world.

I consult to a data center company and we get a lot of these threats. Because we handle their internet addresses, the ransom note actually ends up being sent to us because we are the primary contacts.

We'll receive a fax.

Typically it'll come from an untraceable number, and it will say, you know, at such a time, such a date, we will launch a distributed denial-of-service attack at your site if you don't pay.

If they don't pay, sure enough, at that particular time there will be all kinds of requests.

It could be a very simple request that doesn't even threaten perimeter security, the stuff that Gus talked about.

It could be, say, you require a download of an app in order to place a bet.

They will command their botnets, which could be hundreds of thousands of computers around the world, to download that app over and over and over again.

What happens now is, while your legitimate customers can't download the app, or, worst case, if you have only one ISP, your pipe is now full of all these connections, and everybody else's connections now slow down.

If you wanna bet, you wanna place a bet, you place a bet, you click, you get that spinny thing, and nothing happens.

Mr. Vin Narayanan: Yeah, and so —

Mr. Hai Ng: It kills your business. It actually shuts you down.

Mr. Vin Narayanan: It kills your business. Shuts you down.

What do you need to do to prepare for something like that?

Mr. Hai Ng: The interesting thing about this is that you could have the best perimeter security, and that's not gonna help you because this is essentially something that is brute force.

It stands outside your gate and just prevents people from coming in.

There are ways against it where there's technology that you can place on your network in working with your internet service provider or your hosting facility that will try to distinguish a real customer request from just a fake request.

Then there is technology you can bake in — again, to Gus' point — to plan for this in advance into your transactions so that you could put a certificate into a legitimate transaction portal.

Think of if you call somebody and you're afraid that you might be impersonated, you have a code word.

You pick up the phone and that's something that you always say first. You can build that into a transactions request, and if I'm just trying to do a denial-of-service attack I may not know or may not be able to replicate that certificate, and so now you can tell between a good customer and a bad customer, or a fake customer.

You throw the fake customer requests away and then you let the real customer in.

Mr. Vin Narayanan: Yeah. Anything to add, Gus?

Mr. Gus Fritschie: No. I think Hai made the great points.

In order to really protect against DDoS attacks, you need to really work with your data provider and your upstream providers in order to mitigate those attacks once they start occurring.

Of course, there are ways to do that.

Huge sites out there are big targets, and they've put out those mechanisms, but it does come with a cost, but as you grow in size, once again, that's one of your risks.

You manage your risk.

You're never gonna have a hundred percent security.

Maybe you can live with a certain number of outage, but probably not on Derby day when you wanna be collecting these bets.

It probably is a significant risk and you wanna make sure you have those protection mechanisms in place.

Mr. Hai Ng: Increasingly these days, as well, denial-of-service attacks have become red herrings.

What they will do is they will launch a denial-of-service attack at your site, keep your IT team busy because they're now trying to fail over or trying to restore service, and while you're doing that they're attacking your site.

They're doing perimeter attacks, going to your database because you're not watching anymore cuz your army has been sent to one particular flank, and they're coming in from behind.

Mr. Vin Narayanan: Don't underestimate the business damage that can be done by an attack like this, and I was involved personally in one back in 2003, 2004.

I was working for usatoday.com back then, and we had an attack, a denial-of-service attack that took down our website and it took it down for about eight hours.

It was a lot of work to get that back up and running, and during that downtime we lost ad delivery, we lost money, we lost revenue, we lost click through, we lost audience, and we lost credibility.

Those are all things that you don't wanna lose as a business. I mean those are critical components to a business.

You don't wanna lose that, so it's a serious threat.

Mr. Hai Ng: Not to crank up the scare sauce, but if you're thinking it's hard to attack if you have a big pipe or a big connection and all, it's hard to flood, in I believe it was 2003, the country of Indonesia was DDoS'ed.

The entire country's pipe was blocked. Because it was simply being done by a lot of these botnets that would — your computer today could be infected by a botnet and you wouldn't know it because it's sitting dormant.

A lot of how these botnet happens is they have a controlling computer that will eventually just activate that computer and ask it to send a request to a particular address.

What happened with Indonesia — there was several countries that actually got attacks like that — was their entire connection into the country was inundated with just traffic, just noise, and nobody could do anything.

Mr. Vin Narayanan: Yeah.

No, it's scary stuff, but especially on big days, though, you have to plan for it.

You have to be ready for it.

It goes back to the security session that, if you saw earlier today, have a plan.

Know that this can happen. Have a plan and be ready for it, because it's always a possibility.

Gonna shift gears away from the techy approach to security to something, to social engineering. Was it Mitnick? Kevin Mitnick was —

Gus Fritschie: Kevin Mitnick.

Vin Narayanan: Yeah, Kevin Mitnick, if you don't remember the name, Kevin Mitnick was a hacker extraordinaire for several years, but one of his skills was he was able to socially engineer a lot of his hacking.

What social engineering is — well, Hai, why don't you explain what social engineering is.

Mr. Hai Ng: Social engineering is the — in fact, it's the most popular vector or method of attack for any intrusion security process.

It has no tech associated with it.

It relies on our innate human desire to be helpful and to be nice.

Very simply, it could originate from a call to your tech support, a call to any one of your employees, and they will be very polite. They will sound like they know what they're doing.

Vin mentioned Kevin Mitnick. He has a book that's available out there called *Ghost in the Wire*, and writes about his life.

At one point he was arrested. He was caught. He was arrested.

There was rumors floating around that he could actually launch the U.S. intercontinental ballistic missile system by just whistling into the phone.

That was how much the federal government was afraid of him.

They actually used that line against him in court when they were sentencing him.

What he was able to do was he was really good at a skill known as phreaking, which is spelled P H R E A K I N G.

What that is, is it's phone hacking. He could take over — he knew how to talk to the phone companies. He could get the phone companies to do things for him as if he was a phone company employee.

One of the examples that he did of social engineering was he wanted to steal a password from somebody in Motorola because he was curious at how Motorola phone operating system worked.

He wasn't there to steal.

The interesting thing about Kevin is he never stole anything for profit.

He did it for fun.

He did it for knowledge.

What he did was he had the phone company do a route for him so that when he called somebody inside Motorola, it would actually look like it was an internal call.

He called a low tech person and told her he was IT.

He wanted to make sure that she had changed her password recently because there's been a rash of break-ins, and she said, "Okay," and he says, "When was the last time you changed your password?" She said, "Oh, I've never changed it," and he said, "Okay, do you know how to change it?" She said, "No." Said, "Okay. I'll teach you right now."

He taught her how to change it using the system, changed the password, and while she changed it the first time he logged in from a back door, and after he logged in he told her, "Okay. Now you have to change it back, and don't tell me what it is."

That is social engineering. He won her trust because he didn't want to know her password, but he already knew it because the example that she typed in allowed him in access to the system, and he got in and he got what he wanted and he left. Nobody even knew until he released it.

Mr. Gus Fritschie: Yeah, and what's interesting about Kevin Mitnick is I mean he really wasn't that technical.

He did this all by a typical con artist, gaining someone's trust.

What we see these days when it comes to social engineering attacks, and the ones that we are really concerned about, are those directed — we like to call 'em spearfishing, because instead of these broad emails that go out about —

Mr. Vin Narayanan: Nigerian prince.

Mr. Gus Fritschie: - Nigeria princes, which I think hopefully we all know to delete, it's gonna be something directed.

Let's imagine that Vin worked at a casino, I mean at a racetrack, and on a closed-loop system, perhaps, where no one had — there was no external access but they had internet access in order to receive email, perhaps.

If you were in the previous session, you know he's a big Michigan State fan. If I know that, I can target a very crafted, special email to him.

Hey, Spartans are going to the Rose Bowl.

Click this link to get best prices on tickets.

That could be a malicious link that exploits a vulnerability in his web browser, say some form of Java or something that always has vulnerabilities, and most of the time companies aren't up to date on patching.

There's a much greater chance that he's gonna click on that link than just some random link that you won a prize or something.

How do you protect against this? It's all about user awareness security training. Users are really our biggest weakness when it comes to information security.

Why spend days and days trying to exploit your web application with a SQL injection vulnerability if I can just send an email to the secretary and she's gonna click on something?

Users always click on things.

I have to keep on constantly telling my parents. They call me up, "Oh, my computer got hacked or something. I clicked on this link."

That's how it always starts. Someone clicks on links.

It really goes back to how strong your internal security awareness program is because, when you think about it, even if you have great external perimeter security, even if your website and your application that was providing your racing services was a hundred percent secure, if that person clicks on that link, now that attacker has a back door onto your internal network, which most of the times is not gonna be as secure as your external network because you think, well, who can get to it?

It's my internal network, but you can pivot from that and then keep on exploiting resources.

That's why social engineering is one of the biggest risks out there currently.

Mr. Hai Ng: It's always weakest link in the chain, as you've heard, and we are the weakest link, the human element of it. I mean we talked the previous—the examples that we talked about is exploiting people's willingness to help or people's desire to go get a deal. The get a deal part is the easiest thing to do.

In fact, one of the big vectors that was exposed for a lot of Chinese hackers getting into the networks is they would go to a trade show and they would accidentally drop a lot of USB keys on the floor, randomly scattered once in a while, so you're walking through the parking lot and you see an eight gigabyte USB flash drive. You pick it up.

You think it's your lucky day.

It's a free drive.

You go back, you stick it in. The moment you stick it in, it's in your computer. The vector is in. It loads up. It installs a thing and it goes dormant because a smart — like a biological virus, smart viruses don't kill the host. They stay dormant until they need to work, and even when they're working they try to have little to no symptoms, because then you can run without anybody knowing it.

Mr. Vin Narayanan: Gus, one of the things you brought up was the concept of internal security.

What are some best practices, cuz I mean one of the things — you're dealing with the racing industry here.

You need good internal security, otherwise things can go wrong.

What are the sort of internal security measures that people need to be looking at and thinking about in order to keep stuff out?

Mr. Gus Fritschie: Yeah, absolutely. I think one of the first things that you need to have is resources, internal resources that understand and know security.

I talk to a lot of people in the gaming sector about information security because obviously I'm interested in it. I wanna help 'em out.

I didn't mention on my bio presentation, but I was first a player. That's what got me interested in this whole sector.

I played online poker for many, many years, so I'm very interested in the security of the sites to provide a safe gaming environment, but you need to have a dedicated team that understands security.

Too often, IT even is seen as an expense. It is an expense, and oftentimes you have small staffs that wear many different hats and do many different things.

You may think that you have a — that your security is fine because you asked your IT guy. You're like, "Hey, how's my security?"

"Oh, it's great. Yeah, it's fine."

What do you expect them to say?

In reality, unless they really understand it, it's a totally different training and knowledge than just general information technology.

First, I would say you want to make sure you have either an internal team that can perform the security testing and security design that you require, or you need to make sure you contract it out if you don't wanna have that resource internally.

That's one thing.

Second is you need to know what your risks are.

It all goes back to that.

You don't wanna just cover your eyes and hope that everything is fine. You wanna know what those vulnerabilities are so in order to go about and make business decisions in order to protect them.

That's why I have a lot of clients that come to me and they know — we know we have problems, but we wanna know exactly what they are so we can justify or we can go to management and we can make a case of this is what we need to fix.

This is a consequence that could happen if we don't fix it.

There's a lot, of course, technical details we could get into.

I don't think that's probably appropriate right now as far as what to have from internal security, but that's two things right there.

Have people who can perform those tasks, and then actually do testing to identify those risks.

That testing can be just general network vulnerability assessments from external, internal perspectives.

It can also be focused directly on your applications, your web applications.

Then, of course, your mobile devices. More and more, we see it everywhere. Everything is going mobile.

Everybody wants to be able to bet mobile, and a lot of times developers are thinking that you're device is gonna protect you, when it really isn't.

Devices can be jailbroken, information taken off of 'em.

Those are two key concepts I would say that you want to be made aware of.

Mr. Hai Ng: Gus, have you ever been engaged as like a white hat, and you tell people what a white hat is?

Mr. Gus Fritschie: Correct.

Yeah.

Hai is referring to, in the security industry, there's black hats, which are the bad guys who are going to go ahead and hack your system, and they're not really gonna tell you. They're gonna extract the data.

Then there's white hats, which are companies like mine and several others out there that will go ahead and perform vulnerability assessments, tests on your networks, tell you what those vulnerabilities are.

If you need assistance they'll even help you fix them, or if you have the resources internally you'll fix them yourselves once they give you the advice on how to fix 'em.

Yeah, absolutely.

The best way to know what your risks are is to perform attacks like your adversaries are gonna perform against you. That's really the only way to know.

Mr. Hai Ng: Right. If you were here before lunch on the panel that talked about the bad things hitting the fan, what the gentleman from New Zealand is — you have to run drills, or even just live testing, and you have to do that.

A lot of times, don't have your security tests on a staging system because the staging system is a staging system.

A test on a staging system will only prove how good or bad your staging system is, not your live system.

Mr. Vin Narayanan: That's a good point.

Live testing is really important.

You can only learn so much in a development environment. Hai, one of the things we heard about in one of the earlier sessions, one of the keys to any sense of security is how you respond to an attack.

Mr. Hai Ng: Yes.

Mr. Vin Narayanan: Having a plan and doing that. Go ahead and talk about good ways and bad ways to respond to a cyber attack.

Mr. Hai Ng: Sure.

I think earlier today, you've seen a lot of sessions that basically tell you that the best thing to do is to tell the truth and to tell it fast and address it fast so you can control the message.

No different in a cyber security situation. The worst thing you could do is hide it from your customers if you've got a break-in, because if they — the sooner they know, the sooner precautions that they can take and they can forgive you for that, and you can promise that you're gonna fix it.

The more you tell people, the faster they can react.

Two examples that I can give.

A few months ago, Adobe was attacked. Their system was broken into. Username and passwords were taken. Adobe took an extremely long time to get back to their customers.

In fact, to this day, there are customers that — and analysts, I believe, hasn't been contacted that their account information has been stolen.

This is not just names and password. It includes billing information, which is credit card numbers, expiration date, CCV check numbers.

There are still customers that don't know.

In fact, I know somebody who is a peer of mine in the industry. He does a lot in social marketing. He had an account, was cracked.

Two weeks after the Adobe initial report came out, his credit card was used in Mexico. The number was definitely out there. That's a bad way of handling it.

They were trying to spin control it. I don't know what's happening internally, obviously, but they were taking a long time to do it.

On the other side of the example, we have a company named CloudFire. They're a cloud services provider. They were hacked. Passwords were gotten, and the hacker in that instance was really interesting.

They were targeting one particular person who was a customer of that company specifically. They went through an entire attack structure just to get that person's password, and they succeeded, but what the company did was within less than half a day they had released the entire report of what happened, how the attack happened, a chronological, by time blow-by-blow of what happened and what they're about to do to fix it.

They notified that customer immediately. They shut down his server and they protected him.

The moral of the story is, at the end of the day, you want to protect your customer as much as you want to protect your system.

Transparency, promptness to respond, lets you control the message, similar to a natural disaster situation or a terrorist attack or any form of physical attack.

Mr. Vin Narayanan: I just want to build off the concept of protecting your customer. Gus, you were working on a white paper or on a brute force attack with Ultimate Gaming, right?

Mr. Gus Fritschie: Correct. Yeah. Recently, as many of you may be aware, in New Jersey i-gaming went live.

Was it three weeks ago?

Mr. Hai Ng: Two. Yeah.

Mr. Vin Narayanan: November 26th.

Mr. Gus Fritschie: Okay.

Mr. Hai Ng: Yeah, the week of Thanksgiving.

Mr. Gus Fritschie: Very recently. This can also tie a little bit back to compliance and regulation, because obviously —

Mr. Vin Narayanan: I'll get to that after that.

Mr. Gus Fritschie: Okay. Because in the Division of Gaming Enforcement of New Jersey, there's a specific requirement that they have to make available multifactor authentication to their customers, so instead of just logging with your username and password, once you do that they have to give you another method like, say, send a PIN to your phone, and then you type in your PIN.

That way, even if your username and password was compromised via social engineering or a Pony —

Mr. Vin Narayanan: Yeah, I would have to steal his phone.

Mr. Gus Fritschie: — or the Pony attack, you would still have to steal the PIN. It's great to see these type of additional security requirements being made available, and it's something that we'd probably like to see in the racing industry as well.

It got me curious and I just, I started looking at how they were actually implementing it, and I looked at two different sites.

One site implemented it correctly, and another site implemented this multifactor authentication incorrectly, where if you logged in with the correct username and password, you could then try as many different PINs as possible.

In this case, there was a million different possible PINs, but you could still brute force that, and they were never locking out your account. They didn't have it set up correctly, so you have an example of where —

Mr. Vin Narayanan: Can you just explain the concept of brute forcing?

Mr. Gus Fritschie: Yeah. Sorry. Brute forcing is where you just try the random values.

In this case it was a six-digit PIN, so you could just try all the possible combinations of a six-digit PIN, which is a million possible combinations.

Mr. Hai Ng: Sure, but you would start with 123456.

Mr. Gus Fritschie: Yeah, it would start with 123456 cuz that is the most common.

Unfortunately, it wasn't the PIN they sent me. That just goes to show you how, even if security is implemented, it needs to be implemented correctly.

If you're interested in that, it's on Online Poker Report. There's an article about that.

Mr. Hai Ng: Just to add to that a little bit as well, you also can — security should also be proactive. Like the example I gave earlier, the bad — Adobe being slow to go, there is a proactive silver lining there that somebody took advantage of. Facebook downloaded the — after the hackers compromised Adobe, they actually uploaded an entire file containing usernames and passwords into the open on the internet.

What Facebook did as a proactive security measure, they downloaded that file and they ran that file through their entire Facebook database, assuming that their users could be also Adobe users and use the same email account as their account name.

They would run the password, and if that account succeeded, logged in, which mean basically this user used the same password at both Adobe and Facebook,

Facebook locked out their account, sent them an email and said, look, your email was — your account was compromised at Adobe, and we discovered that you used the same password, so to protect you we've locked out your account.

Please change your password.

Mr. Gus Fritschie: Yeah, and that's a great example of a company being proactive and protecting your customers and users.

I wanted to make this point when Hai was talking about social engineering.

We were focusing on attacking the employees of your organization, but the same applies to your customers, because if your customer gets phished and they get malware installed on their computer that allows someone to break into their online horse racing account and maybe place a bunch of bets that they didn't want to have placed, even though really it's not your fault, it's still gonna come back.

Well, my account was hacked on Xpressbet or Derby Wars or whatever. You wanna make sure that you give your customers information and encourage them through proactive policies in order to be secure.

Mr. Vin Narayanan: That's one of the points I wanted to get back to, was the concept of securities actually protecting your customer.

By fixing the vulnerability that you found from the brute force standpoint of fixing the PINs, you've just prevented their account from being hacked, or made it much more difficult to be hacked. That's, in essence, what you're doing is you're — the security is protecting your customer. The cyber security is not only protecting your company and your company's reputation, but you're also protecting your customer.

One of the things that's come up here is the idea — and Gus mentioned the fact that DGE New Jersey, Department of Gaming Enforcement, requires multifactor authentication, which is a password and then a second form of authentication to log onto account, but just because a regulator asks you to do something, complying with them doesn't mean that that's the end of your security responsibility.

Because what regulators ask you to do is do the bare minimum.

In this case, multifactor authentication. Ultimate Gaming did the bare minimum, but you wanna know what, their system still wasn't secure.

Mr. Gus Fritschie: No. Yeah, absolutely.

This goes back to compliance.

A lot of my business comes from compliance, so I really shouldn't be up here bashing compliance. I mean I do a lot of PCI work, a lot of FISMA work in the federal government, and you get many, many companies and organizations that have met compliance because they have to. They have to check that box. A lot of times, they spend more money and effort checking that box than they do really securing their system.

My message is, is that while, yes, you're gonna need to comply with certain security regulation and standards, be it unique to your industry or more standard like PCI, or if you get ISO compliance, et cetera, et cetera, you don't want that to be the end all, because there is plenty and plenty of examples of companies that were PCI certified and then suffered massive credit card breaches.

I would like to see security regulations strengthened in order to make operators and sites adhere to more stringent policies.

That's an uphill battle, but I think what we see in DGE in New Jersey is a good start.

You can argue it's stronger than what was placed in Nevada, which was the first state to have online gaming, but my message is compliance isn't security, but it's a first step in order to getting to security.

Mr. Vin Narayanan: All right. Before I ask any more questions, let me ask for questions from the audience cuz you actually have some security experts here. You might as well take advantage of their expertise. Everybody is secure.

[Laughter]

Audience Member: Nobody is secure.

[Laughter]

Audience Member: Quick question for you. A number of years ago, the offshore sports books, when the Green Mail attacks were happening against them for the DDoS, lots of them signed up with Prolexic and companies like that.

Prolexic obviously built that into a multimillion dollar business and sold out. Are companies still doing that? Is that the primary form to guard against the DDoS attacks?

Mr. Hai Ng: Yes, that is the main form still.

It's traffic cleaning, clean pipes, which is what Prolexic does. Let me just, for those that you don't know how that mechanism works I will just quickly run through it.

You basically buy an insurance policy from Prolexic. They run a connection to you. If you get attacked, you divert all the traffic to them. They have technology that will try to discern actual traffic and attack traffic, and they do that by profiling your traffic during a non-attack, so they kind of predict what your traffic looks like. Things that look right, they will send along to you.

Things that don't look right, they will just route into what's called a network black hole and it would just disappear.

Companies like Prolexic do that. The hosting company that I do consulting work for, called Continent 8 Technologies, they do a lot of i-gaming and gaming services.

They have internal technology supported by Arbor Networks that do that.

Cisco used to do it. They don't do it anymore. They've left that business, but it's a very vertical market business and, yes, technologies like that, in essence, is pretty much your only defense apart from having a very, very big bandwidth connection.

Mr. Gus Fritschie: I agree.

Mr. Hai Ng: Yeah.

Mr. Vin Narayanan: Any other questions? All right.

I've got a question going back to compliance for the both of you.

Can you come up with an example or think of an example after we had the ultimate gaming one where the compliance standards offered a minimum sort of thing, but it was way below what you thought was reasonable for that sort of security?

Mr. Gus Fritschie: Yeah, sure.

No, I can give another example of the New Jersey regulations. They do require some type of security test.

I think actually in the regulation it says on an annual basis, the operator needs to perform an independent security test, but that's all it really says. There's so much variance in what security test means. Does it mean just running a basic scan against the website and saying, yes, you're secure?

In fact, when it comes to PCI compliance, part of it is you need to have quarterly scans done against your website by a ASV.

All they do is run a basic scan against your website. If they don't have real credentials, they're not logging into your website. They're not really gonna find any vulnerabilities.

Or is it something more? I mean that piece of the compliance regulation could spell it out in more detail referencing a body of knowledge like OWASP or something else in the security industry that should be done according to these standards.

Rather, it just leaves it broadly for the sites to interpret, and unfortunately a lot of the sites, they wanna do what costs the least amount of money. If they can get away with doing the less, that's what they're going to do in a lot of cases. That's not to say everybody.

There's a lot of sites out there that are very proactive, that go above and beyond what the security regulation calls for.

PokerStars is a good example. From people I've talked to there, they actually take security very, very seriously and do a lot more than what is required by their regulatory bodies.

Mr. Hai Ng: Well, here's an example for outside the gaming industry.

Both Google and Facebook provide rewards for any white hat that is able to compromise their security in any shape or form. Google will actually pay you, I think at one point it was $3,141, which is pi for those that know what it is.

Mr. Vin Narayanan: I was wondering how you knew the exact number.

Mr. Hai Ng: Yeah. Facebook will do it as well. They have rewards.

Mr. Gus Fritschie: Some might argue that that's actually cheaper for them to do, even hire a professional company to come in and perform their security service, but by offering these bug bounties, but no. They definitely do attract some attention from white hate researchers who notify them of vulnerabilities.

Mr. Hai Ng: It's a great way for white hats to gain some reputation, too. If you're starting out in industry, you're getting somebody who will pay you and publicize your name that you did it.

Mr. Gus Fritschie: Yeah. I guess my advice also is, if you do — and I'll do this occasionally, like in this ultimate example, I wasn't hired to look at their website. I didn't do anything illegal. It was my own account that I brute forced, so I wasn't trying to break into anyone else's account, and notified them of the results of it, and they've taken steps to mitigate it.

If you are operating a site and you do get approached by someone, it's not like they're trying to blackmail you. A lot of times people are out there and they're looking for these things just because there's a lot of people in the information security community who do wanna help, who wanna make sites secure.

That's our job.

We wanna make sites secure.

If you do get that, hey, it's free.

Take that advice and go and secure it.

Mr. Hai Ng: That's actually a good point. Take that advice. Don't dismiss them. Don't dis 'em, for sure, because they're just gonna go public with it.

Mr. Gus Fritschie: Yeah.

Mr. Hai Ng: It's better that you talk to them and work with them to figure it out. If somebody calls you up and say, "Look, I just cracked your system," don't hang up.

Mr. Gus Fritschie: It might be a sign that your security really does need to be looked at, and, to be honest, that's why I do look at some of these different sites.

I'm trying to make a point that security is a concern in this sector, because it's my belief that a lot of people aren't viewing it as a major issue, and I want to raise awareness that there are issues out there.

That's why, if you saw in my slides, it was less than an hour of just me looking at traffic going back and forth between my web client and the web server and noticing some of these trivial vulnerabilities.

You can imagine if these trivial vulnerabilities exist, what else is out there?

Mr. Vin Narayanan: What Gus and Hai just said, though, about if someone comes up to you, sends you an email, walks up to you and says, "Hey, I noticed this vulnerability in your system," take it seriously.

Don't ignore it, because what's gonna end up happening is investigate it.

Make sure that that vulnerability either doesn't exist or exists, but don't ignore it, because if you ignore it and it exists, it's gonna get publicized.

Because they're gonna go to someone and say, "Hey, I told them about this. I told them about this vulnerability. They didn't take it seriously. Now I'm posting it for the world to see."

If you investigate it and you determine, yeah, it's not there, all right. You just check to make sure your systems are more secure, and if you investigate it and you find out the vulnerability is there, then now you have an opportunity to fix it.

Mr. Gus Fritschie: Yeah, and unfortunately that's what happened with healthcare.gov.

I mean there were some independent security researchers out there that once the site — you might argue it was due to political motivations, perhaps, but there were people who were looking more closely at that site and discovered vulnerabilities that probably should have been discovered before the site went live.

They went public with it, and they forced their hand.

In fact, there was a whole hearing where one of these security experts testified in front of congress about what he found just doing basically what I did here in my presentation.

Mr. Vin Narayanan: All right. We're at the end of our time here, but just really quickly, two takeaways from each of you that the audience here should think about security as they walk out of the room.

Mr. Gus Fritschie: My two takeaways would be don't dismiss that it's not a problem that it's not your concern, and also to go about and test and know what you're risks are.

Mr. Hai Ng: The best person to formulate a strategy for you in terms of security is an optimistic pessimist.

Mr. Gus Fritschie: All right.

Mr. Vin Narayanan: I will leave you with that conundrum. Just wrap your head around that. It's actually true.

With that, I wanna thank our panelists here.

They did a fantastic job, and I wanna thank all of you for listening.

Thank you very much.

[Applause]

Mr. Hai Ng: Thank you.

Mr. Gus Fritschie: Thank you.