REFINITIV STREETEVENTS

EDITED TRANSCRIPT

INTZ.OQ - Q4 2020 Intrusion Inc Earnings Call

EVENT DATE/TIME: FEBRUARY 25, 2021 / 10:00PM GMT

©2021 Refinitiv. All rights reserved. Republication or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. 'Refinitiv' and the Refinitiv logo are registered trademarks of Refinitiv and its affiliated companies.

REFINITIV

CORPORATE PARTICIPANTS

Franklin Byrd *Intrusion Inc. - CFO*

Jack B. Blount *Intrusion Inc. - President, CEO & Director*

CONFERENCE CALL PARTICIPANTS

Howard D. Brous *Wellington Shields & Co., LLC - Broker*

Porter Ross Taylor *ARS Investment Partners, LLC - Partner*

Zachary Cummins *B. Riley Securities, Inc., Research Division - Analyst*

Joel William Achramowicz *Shelton Group - MD of IR*

PRESENTATION

Operator

Good afternoon, and welcome to Intrusion's Fourth Quarter 2020 Financial Results Conference Call. (Operator Instructions) As a reminder, today's conference call is being recorded for replay purposes. I would now like to turn the call over to Joel Achramowicz of Shelton Group Investor Relations. Joel, please go ahead.

Joel William Achramowicz - *Shelton Group - MD of IR*

Thank you, Rob. Good afternoon, everyone, and welcome to the Intrusion's Fourth Quarter and Full Year 2020 Earnings Conference Call. I'm Joel Achramowicz, Managing Director of Shelton Group, Intrusion's investor relations firm.

Joining me today are Jack Blount, Intrusion's President and CEO; and Franklin Byrd, Intrusion's new CFO.

Before we begin the call, I want to remind you that today's conference call may contain forward-looking statements regarding future events, including, but not limited to, expectations for Intrusion's future business, financial performance and goals, customer and industry adoption of Shield technology, successfully bringing to market Intrusion's design pipeline and executing on its business plan.

Now these forward-looking statements are based on estimates, judgments, current trends and market conditions and involve risks and uncertainties that may cause actual results to differ materially from those contained in the forward-looking statements.

We encourage you to review the company's SEC filings, including the 2019 Form 10-K we filed with the SEC on March 27, 2020, and other SEC filings made from time of time in which we may discuss risk factors associated with investing in Intrusion.

All forward-looking statements are made as of the date of this call, Thursday, February 25, 2021. And except as required by law, we do not intend to update this information.

This conference call will be available for audio replay for at least 90 days in the Investor Relations section of Intrusion's website at www.intrusion.com.

I will start the call off with a review of the financial results by Franklin, and then Jack will review Intrusion's recent operating developments progress with Shield and the company's key objectives going forward. Then we'll take your questions.

And with that, I'd like to turn the call over to Franklin. Franklin, please go ahead.

©2021 Refinitiv. All rights reserved. Republication or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. 'Refinitiv' and the Refinitiv logo are registered trademarks of Refinitiv and its affiliated companies.

REFINITIV

Franklin Byrd - *Intrusion Inc. - CFO*

Well, thank you, Joel, and thank you to everyone on -- who joined us today. As you know, this is my first call as the CFO, and I'm excited to be on board. I look forward to meeting with you in the coming weeks and working closely with Jack and the team during this exciting time at Intrusion.

So turning to the fourth quarter 2020 results. Revenue was $1.6 million compared to in $1.6 million in the prior quarter and $2.6 million in the fourth quarter of 2019. Revenue for the full year 2020 was $6.6 million compared to $13.6 million in the prior year.

2020 revenue for the fourth quarter and the full year were impacted by extended government shutdowns related to the pandemic, which delayed subscription renewals and contract starts for our government business. However, as we indicated in the recent press release, we've begun to see signs of recovery on our government business, and we see those continuing to levels that we've seen historically. Additionally, 2019 revenue for the fourth quarter and the full year benefited from 2 onetime contracts that were unique to 2019 only.

Gross margins in the fourth quarter were 58.2% and as compared to 58.9% last quarter, and 61% in the fourth quarter of 2019. For the full year 2020, gross margin was 59.1% compared to 60.8% in 2019. Operating expenses in the fourth quarter were $4.8 million, which included a $1.1 million noncash write-off related to a prior office lease agreement. This compares to $2.3 million last quarter and $1.3 million in the same quarter a year ago.

Full year 2020 operating expenses were $10.4 million, which includes the same $1.1 million noncash write-off just mentioned and compares to $3.8 million in the prior year. In addition to the $1.1 million noncash write-off in 2020, we had year-over-year increases in operating expenses for 3 or 4 primary areas. Number one, the hiring of 31 additional employees across the board for development and launch of Shield. The breakdown of these in our hires are 20 in sales and marketing, 8 in research and development and 3 in general and administrative areas.

Additionally, we stepped up marketing efforts in the second half of 2020 in preparation of our Shield launch, and we increased development activities for Shield and future solutions offering. And to a lesser extent, we had increased registration expenses related to the October stock offering and our move up to the NASDAQ.

Net loss for the fourth quarter of 2020 was $3.9 million, which included the $1.1 million noncash write-off related to the prior lease agreement. This compares to a net loss of $1.4 million for the prior quarter and net income of $0.3 million in the fourth quarter of 2019. For the full year 2020, the net loss was $6.5 million, which also included the $1.1 million noncash write-off in the fourth quarter and compares to net income of $4.5 million in 2019. After the pool of preferred dividends, the net loss attributable to common shareholders in the fourth quarter was $0.23 per share on 17 million shares compared to a net loss of $0.10 a share in the prior quarter and net income of $0.02 per diluted share in the same quarter a year ago.

For the full year 2020 after the accrual of preferred dividends, net loss attributable to common shareholders was $0.45 per share compared to net income of $0.28 per diluted share in 2019. Cash and cash equivalents as of December 31, 2020, was $16.7 million compared to $1.5 million in the prior quarter, reflecting the $18.2 million in net proceeds from our successful follow-on offering that closed in October.

Working capital was $16.2 million and total outstanding debt at the end of the quarter was $633,000, including the current portion. In terms of guidance, we will not be providing quarterly guidance on today's call. As you know, we're still in the early stages of ramping up our orders on Shield. It's very, very difficult to accurately predict the exact timing of the revenue ramp up. However, we do want to reiterate that we're extremely encouraged by the high level of interest and the demand in such a short period of time since launching the Shield to the market, and we expect to continue the strong momentum into the coming quarters ahead.

Now I'm pleased to pass the call over to Jack to review recent business developments with Shield and several other activities in the company. Jack?

Jack B. Blount - *Intrusion Inc. - President, CEO & Director*

Thank you, Franklin, I appreciate you giving that cover for us, and thank you all for being on the call today.

©2021 Refinitiv. All rights reserved. Republication or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. 'Refinitiv' and the Refinitiv logo are registered trademarks of Refinitiv and its affiliated companies.

REFINITIV

We are extremely excited about the reception that Shield has gotten in the marketplace since we launched it and the progress that we're seeing in the field. I can tell you that the product continues to perform near perfect. As one of my prospects, as I was quoting in some of our data actually quoted back to me in a call earlier today, our numbers show that we are 99.999% accurate every time we make a decision about whether we kill a connection or not. There is no product on the planet that can get close to 3 9s, much less 5 9s. Most firewalls, most cybersecurity products actually tell you they have a 30% error ratio. So we are orders of magnitude on the other side of this equation compared to any other technology.

Again, I draw you back to what makes Shield so unique and so valuable, and I'm not sure that people, even though we've talked about this many times, have fully picked up on it, so I'm going to restate it this morning -- excuse me, this afternoon. Shield is really all 3 of Intrusion's technologies married together in a single product solution. The TraceCop database that we have created, managed, grown, used for 25 years, is the core of what makes Shield work today. Everyone asks me all the time, how can our AI be so much more accurate than any other company's AI in the world. The answer to that is understanding AI.

AI is 2 things: it's mathematical algorithms that teach computers how to learn. But that's actually a very small piece of the equation. What AI is really about, as Google will tell you and says all the time on the news, and Amazon says all the time, AI is about data. If you have a massive amount of data, then AI can learn any and everything there is to learn. If you don't have enough data, you can't learn anything. In fact, you'll learn false truths. The reason our AI is so brilliant is we have the only 25-year-old hundreds of petabytes of data of Internet traffic and malware for 25 years, that our AI studied to learn from so that it's as smart as it is, and it can have 5 9s of accuracy, and we think we can take that to 6 9s shortly. We're working on improvements right now to do that. I want it to be near perfect.

So the TraceCop database, which this company has developed for 25 years, is the core of why this product exists and why it works. Equally important is the Savant product. We have had the Savant product in production for 12 years. It's on release 16, I think, if I remember correctly.

The ability to open real-time, every packet of data coming on or going off your network is a patented, unique and valuable technology. For example, you may or may not realize, most firewalls only open 10% of the packets coming on to their network. They pass 90% of them without looking at them because if they try to look at all 100% of them, they would slow your network down too much and you wouldn't use their product.

We can actually open every packet and not slow your network down. So the Savant technology that we've had and improved for 12 years, again, is a core piece of the technology of Shield. How we open, inspect every packet of data is with the Savant technology. The only new thing that there is in Shield is the artificial intelligence that learn from the database, that can interpret what it finds when it opens a packet of data, and how it can decide if it's good or bad, when humans could look at that packet of data and have not a clue whether it was normal traffic or not normal traffic.

AI can tell you, as we're proving with 5 9s of accuracy, whether that's good or bad data. So you have to think about Shield as the combination of 25 years of R&D, 25 years of product and development, 25 years of expertise around cybercrime, combined into a single product that works as the only -- I'll say again, the only cybersecurity product on the planet that real-time opens every packet of data coming on to your network or going off of your network, inspects it and makes a decision as to whether it passes it or kills it in real time. Not later, not by somebody looking at an alert, not by studying logs later, but real time, it happens. And it's 5 -- got 5 9s of accuracy. And again, as I've told you before, in that rare occasion that we would kill a session that an employee feels is valuable and necessary for them to do their work, they can real-time, override the computer's decision to kill that session and reactivate it and continue working. So an employee is never going to be bothered by our technology.

Now how we can do that is by the fact that while we say we're going to trust it temporarily, we're going to let that employee connect, we then send that request up to our supercomputer to be looked at by our master AI. So what you can do at the millisecond second speed level is far more limited than what you can do if you have an hour or 2 to analyze it. So when we send that up to the supercomputer, it'll analyze it. If it comes back and says, yes, this is a safe connection. We should have allowed this. We know why the client thought this was not safe. We're going to now deem this as approved. We'll never block it again. The employee will never get that message again, and everything goes on as working.

If on that rare occasion that 100th of 1% of a time that were wrong, and we decided, no, this is really bad, it should have been blocked, we immediately re-disconnect that connection. So that connection's probably still going on with that employee. We go back in, we immediately terminate it and we never allow it to connect again. We actually call the IT department and tell them that we've done that and tell them that -- why we've done it.

©2021 Refinitiv. All rights reserved. Republication or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. 'Refinitiv' and the Refinitiv logo are registered trademarks of Refinitiv and its affiliated companies.

REFINITIV

Therefore, we're keeping your network safe even while allowing you to override our computer decisions during those rare exceptions. That way, we can be near-perfect in everything we do, employees can do everything they need to do.

Now why do we sometimes kill a session that's actually good? 99% of the time, that's a brand-new URL that we haven't had time to learn about yet, that just had introduced maybe on the network that day that some employee knows about and is now using it. So therefore, he thinks it's safe because he knows it's new. So that's how that happens and why that sometimes comes up. But together, the technology allows us to have 5 9s of accuracy and still keep employees happy and functioning without disrupting them.

So I hope you don't mind me taking a minute to explain that. But again, I talk to a lot of you at various times during the month and I hear things coming back to me and say, yes, they really still don't understand how Shield works and why it's different. I better make another pass at that.

So let's get back to the pipeline. Again, 2 months, we have seen the pipeline go from 0 to Fortune 100 companies that have our product in trial right now in their labs; Fortune 500 companies that have our Shield installed in their network, testing it; mom-and-pop companies that have Shield installed in their network and testing it; government agencies, both federal and state who have Shield, installed and are evaluating it.

So our pipeline has gone from 0, January 4, to very large with very significant customers in all markets of all sizes in just 2 months. I have 42 years of selling technology in this industry, I have never seen the launch of a product generate a pipeline this dramatic this quickly. So while I can't give you more details on it right now, I certainly want you to have confidence that our salespeople are as busy as I am. There's nobody sitting around that's not actively doing something because the demand is out there.

And how are we going to get even more demand? Well, let me just point out a couple of significant things that have changed that are very, very important to me. I have been fortunate enough, after looking for some time to hire what I think is one of the top chief marketing officers in the industry, Gary is our new CMO. Gary came to us just this week. So I hired -- Gary Davis, by the way, is his full name.

Gary comes out of Intel and McAfee. Gary has 15 years of experience in the cybersecurity industry at Intel and McAfee. His knowledge, his customer relationships, his experience with marketing, his understanding of MarTech and how you really generate warm interested viewers on your website is the best I've ever come across. When I found Gary, I felt like it was a message from heaven. I really felt blessed to have found Gary, to be able to recruit him to our team. He started Monday of this week, he has been nonstop every day this week. He comes to work every morning as excited as I am. He is having, he says, the time of his life. I'm sure he's listening on the call this evening with us.

In addition to adding Gary, which really completes and fills out our management team, you really can't have a technology company dealing in a complex, intense competitive space as cybersecurity without having a Chief Marketing Officer. So to be able to step up and add that level of character to the team is huge for us. And that's why I wanted to spend a minute talking to you about it. Again, I am very, very excited and pleased to have Gary on the team. He and I work together, like we've known each other, our whole lives.

In addition, we announced that we added a Board member very recently. And again, I am very, very excited about talking to you for a second about Katrinka McCallum. Katrinka comes to us out of Red Hat Linux, one of the fastest growing, most successful technology companies in the world. I have tremendous respect and confidence in the Red Hat Linux technology and the work that Katrinka has done to help grow that company from a start-up years ago to a $3 billion annual company last year and get acquired by IBM for, as I'm sure you know, billions of dollars, is a huge success to her and to her management team at Red Hat. And to, therefore, be able to pick her up and add her to our Board of Directors, is a huge win for us.

Not only does she have the broad experience of an operating system such as Red Hat Linux, with international customers and distributors and partners, but she used to be the VP of a software company that did cybersecurity before Red Hat Linux. So she does understand cybersecurity far more than most executives even in technology company. So I think Katrinka is going to be an extremely valuable asset to us here with the team. She broadens us from the broad and historic financial Board of Director-type members we've had in the past with this company, to really be in a commercially based public company, new technology participant. So I think Katrinka is going to be a great resource to me. I am very, very excited, again, to take a minute to talk to you about how lucky and how fortunate I feel to have found her and to convince her to join our company.

©2021 Refinitiv. All rights reserved. Republication or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. 'Refinitiv' and the Refinitiv logo are registered trademarks of Refinitiv and its affiliated companies.

REFINITIV

And in that vein, I would just go ahead and share with you, as I think I've said before on these calls, my intent is to grow our Board of Directors. Our company has gone through a major transformation from being a DOD specialized consulting entity to a commercial solutions offering, and that brings our need to have a broader set of board members than strictly financial, which was the company's history. So I will be looking to add another Board member or 2 to broaden us, to bring in the skills we need.

For example, one of the things that you would obviously expect me to be looking for, that I am looking for, I've interviewed several already, is someone who has been a formal CISO, a Chief Information Security Officer. I want a Board member with that background to be sitting at the Board with me and helping, advising me and to help grow this company into the future. So one of the things I continue to work on -- while I think the management team is complete, I am going to continue to grow our Board of Directors to be a broader set of skills that this company needs given where it's headed today and where we are.

So again, with those significant enhancements, I think those are dramatic growth factors for our company that's going to help transform us and help accelerate our rate of growth. With that, let me just say that again, I think that the market is the largest market in the world, 34 million businesses in the United States alone, 90 million businesses worldwide. All of those businesses can and should be a customer a Shield. Every one of them uses the Internet commercially, every one of them, therefore, is subject to cybercrime. Many of them, if not most of them, have already been breached at least once. It is not uncommon for me to talk to a company that's been breached 3x in the last 3 years. That's how severe cybercrime is today. Literally every 3 seconds of every day, a business somewhere in the world was breached by cybercrime. That's ongoing, nonstop every 3 seconds.

The SolarWinds breach from November, December should have been a wake-up call for the world of how bad cybercrime has become. It is growing at an accelerated rate like nobody could envision. It's hard, if not impossible, to calculate the total losses to business from cybercrime. The number that's commonly used, and I think it's extremely small, is $3 trillion in verifiable losses to cybercrime last year alone. And the estimate is $6 trillion will be lost this year, and I think when you look at Internet intellectual property, customer list, credit card information, source code as well as ransomware that the number is actually much, much larger than that.

What we see, what we track and what we know by our database through TraceCop, our Savant deep packet inspection and our AI tells us that a minimum of 12% of all Internet traffic is malware today. I have seen estimates as high as 32% of all Internet traffic today may be malware. Again, as you remember, from our early customers we talked about, in just 3 months and just 12 businesses, we killed 77 million malware attacks. The problem gets bigger every second of every day. It's an extremely profitable business. Almost nobody ever gets prosecuted for cybercrime. It's not like robbing a bank, there's no risk. You're not going to jail. You're just getting free money from somebody else, and that's why it's growing so fast and that's why so much money is being spent on it.

One report that I saw, 4 -- no, 5 years ago, actually showed that a cybercrime organization that was shut down successfully by the FBI and other international agencies that were involved, was actually spending $100 million a year in R&D, developing new malware agents. These are not kids, these are not just cybercriminals, these are companies, organizations with PhDs, with scientists, with supercomputers that are disrupting the world.

One multi-billionaire who is quoted in the paper all the time, recently said he believes cybercrime is a greater threat to humanity, not just business, to humanity than nuclear weapons. That's Warren Buffett, if you haven't read that quote. Warren Buffett, a businessman, not a cyber engineer, not an engineer, period, just an insanely successful man who owns well over 100 businesses, realizes how dangerous cybercrime is, and that's why he made that statement.

So I don't think we could be in a better place in the market. I came out of retirement because I have an insane passion for stopping cybercrime. I believe we have invented the only technology on the planet that can continue to effectively stop cybercrime every second of every day. That's why I'm here. That's why I'm hiring the best minds and the best people in the world. That's why we have the best AI engineers, and that's why our product gets better every second of every day.

With that, I think we can open up to questions. Is that right, Joel?

Joel? Moderator?

©2021 Refinitiv. All rights reserved. Republication or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. 'Refinitiv' and the Refinitiv logo are registered trademarks of Refinitiv and its affiliated companies.

REFINITIV

Joel William Achramowicz - *Shelton Group - MD of IR*

Please queue up for questions.

QUESTIONS AND ANSWERS

Operator

(Operator Instructions) And your first question comes from the line of Zach Cummins from B. Riley Securities.

Zachary Cummins - *B. Riley Securities, Inc., Research Division - Analyst*

I appreciate the commentary around the opportunities for Shield ahead. Jack, I know after your beta tests have completed at the start of this year, it sounds like a majority of those customers have went on and became actually paying customers for Shield. Is there any way you can kind of quantify the opportunity there, just within the beta participants, just to give us a sense of the potential seed opportunity?

Jack B. Blount - *Intrusion Inc. - President, CEO & Director*

Well, we have not given public numbers. As I've said many times, cybersecurity customers are very, very, very reserved about disclosing who they are, what they'll tell you about them, because they believe any information they give the cybercriminals, they give them more opportunity to effectively attack them. Now we have done 3 -- 2 studies on 3 of those customers. So there is public information by names of those customers and 3 of those companies that are using the technology. We are working with other beta customers -- former beta customers, to also get them to release case studies. We think we're going to get most of them to release in the next 30 to 60 days. So we are trying to get more data out there.

I can tell you, as we said before, 90% of our beta customers became paying subscribers on the Shield product. I would have liked to have had 100%. I've never before, in my history, seen a company accomplish 100% of beta customers. In fact, I can't really find a company that had 90% of their beta customers convert. So I think that's a very, very impressive number, that we were able to do that. I can tell you that one of our former beta customers, which is now a purchasing beta customer, is using the product at multiple locations here in the United States and is rolling -- planning to roll out, as soon as we get approval, in 6 foreign countries.

They are a worldwide business and they want to be protected worldwide. They want Shield running in every one of their offices around the world. So they are simply waiting on us to get federal approval to be able to export the product, which I think we will have by the end of the quarter. The lawyers, right now, are telling me thumbs up. We're getting every check box from the government, we're going to get this done very quickly.

And that's very, very exciting because the international demand, even though we're spending nothing to advertise, promote internationally, we are getting a tremendous growth of inbound request in France, in Germany, in the United Kingdom, in Africa and Latin America. I mean we -- the interest internationally is really, at this point, mind boggling. We have resellers that are begging us to let them sign up to be resellers, even though we can't ship internationally yet. So the demand internationally, I think, is extremely high.

So we have not given out seat numbers and we have not given out revenue numbers on our customers to protect their privacy. You can work backwards from that, by the case studies, by looking at the size of the companies and get some of that information that way. We will, as the company grows and as people get more comfortable, make more public information about the number of seats. Certainly, our revenue each quarter will be a back -- a way to back into that. But right now, companies are very, very reserved about wanting to reveal that kind of information.

©2021 Refinitiv. All rights reserved. Republication or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. 'Refinitiv' and the Refinitiv logo are registered trademarks of Refinitiv and its affiliated companies.

REFINITIV

Zachary Cummins - *B. Riley Securities, Inc., Research Division - Analyst*

Understood. And then speaking on the distributor and retailer front, I know you can't do it internationally, but I mean, can you speak to the progress you've seen with signing up distributors and resellers here domestically?

Jack B. Blount - *Intrusion Inc. - President, CEO & Director*

We have 16 under contract as of this phone call. We have 42, in total, that are in process that I think will have signed up by the end of Q1. So that is going as fast as the other pipeline. Again, it's close to opening floodgates. People are learning about the company. They're learning about the technology and they're wanting to sign up. So I think that's going extremely well.

We should have, I think, starting next week -- we are doing a lot of rework on our website right now to make it dramatic better, and one of the things we're going to be adding is who those resellers are, how to get ahold of them. They will be on our website very shortly. So we will be adding nationally. You'll see that list as they come there. And as we add them, you'll see the list continually grow. So that should be dynamic on a week-to-week basis. As they sign up, once we get that launched here, I hope -- I think, in the next week.

Zachary Cummins - *B. Riley Securities, Inc., Research Division - Analyst*

Understood. And I appreciate the commentary kind of you outlining the pipeline. I mean, I know you can't give kind of specific seat quantities, but I mean, can you outline or even kind of quantify what some of these potential opportunities could look like at either some of these major enterprise customers? Or some of these federal government agencies?

And I guess the second part of that question is, do you get paid as some of these companies are testing out the solution? It sounds like you're already in the door with many entities on that front.

Jack B. Blount - *Intrusion Inc. - President, CEO & Director*

We are not charging for evaluations. We might do that at some point. That's something I never liked doing at any company I've been at. I just feel like it's kind of a requirement of the complexity of the technology we deal with today to give customers that ability to get their hands on it, especially a product as unique as ours. I mean, you listened to what I had to say about the product. It's very, very easy for anybody to say, "Sounds too good to be true, Jack. I've heard that before." So I understand that. It does sound too good to be true. I've been in cybersecurity technology for 42 years. I designed and invented this product, and I think it's too good to be true.

So I give them a free evaluation. They have to go through a qualification to show the size of the opportunity, the level of executive commitment in their organization, their ability in their budget to fund it, before I'm going to send them hardware. But we are doing that without charging them today. I should have -- and again, I'm sure it's hard for you all to understand how busy one CEO can stay, but I'm extremely, extremely busy. If I'm not visiting with customers, or resellers, or distributors, then -- and I'm not recruiting somebody, it's just unbelievable.

One of the things I planned to prepare for today and I just ran out of hours and the fact that it just didn't stay in the front of my mind, is that I wanted to develop a list with some more information for you on that, and -- so I'll get that out to you shortly. But again, I think the pipeline -- again, I can tell you I have a Fortune 100 -- more than 1 Fortune 100 company that's evaluating the technology right now. That single -- any Fortune 100 company could be anywhere from 100,000 seats to 0.5 million seats. That's just the nature of a Fortune 100 company. Any -- pretty much any federal government agency can be 50,000 and up. So any one of those are elephants that will change everything about this company overnight.

Our target was not to go after these big boys because they're generally slower to decide and they can drag you along, but we're just -- we can't not pick up the phone, and that's where some of our highest interest has come from. Midsize, certainly, we have companies of every character all across the company -- all across the country that fall in that 100 to 500 seat range, and I think we're going to see many of those come online. Some of those in Q1, lots of those in Q2 because they just take less time to make decisions.

©2021 Refinitiv. All rights reserved. Republication or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. 'Refinitiv' and the Refinitiv logo are registered trademarks of Refinitiv and its affiliated companies.

REFINITIV

So the pipeline is growing. Every day, it gets bigger. Again, I think the things Gary will be able to do from a MarTech standpoint to bring more warm leads to us, to bring more eyeballs to our website -- again, he's doing a completely new website for us that'll generate more traffic, that this -- the pipeline's just going to grow rapidly.

Zachary Cummins - *B. Riley Securities, Inc., Research Division - Analyst*

Yes. Understood. I appreciate the additional color on that. And as far as the development side, I mean, you've mentioned some of the other products that we could be expecting for Shield here in the upcoming months, including either cloud or even kind of a remote worker capability. Can you give us an update on the development progress there? And when we could be expecting some new releases?

Jack B. Blount - *Intrusion Inc. - President, CEO & Director*

Well, we are -- the 2 products we are really focused on working on is the remote worker. Now again, we handle the remote worker much better than people understood we did before. So if a remote worker uses a VPN to connect into their corporate network, then they are automatically protected by Shield today. And what we are finding is, we -- to be honest, we haven't found a customer yet that comes to us that is not using a VPN.

So the need for a specific remote worker products may be a lot less than we thought it was, so we've actually -- I've actually pulled some resources off of that project until we learn more about the market opportunity and whether it's justified or not because we're just not finding companies calling in and saying the remote workers are not using VPNs. Much more than I expected, every company that went remote with COVID was apparently smart enough to force those employees to use a VPN, which makes them automatically part of the network and protected by Shield.

So that product seems to have a less importance to us than we thought it was going to have. As a result, again, we're a limited size company, we have limited resources. I have pulled some of those resources on to some other things and -- while we track that opportunity.

The cloud, again, I think, was a huge misunderstanding, and I'll take the blame for that myself. Initially when we launched the product, there's 3 different cloud segments that have to be looked at. It's not just cloud or no cloud. According to Gartner and Forrester, 70% of cloud customers today operate in either a private or a hybrid cloud environment. Again, like the VPN client, Shield today works perfectly normal and fine in a hybrid or private cloud implementation. We, ourselves, here at Intrusion, run out of a private cloud environment, and we certainly use Shield running in our own private cloud, protecting our employees around the country.

So again, when you look at the cloud market and understand that 70% of it is hybrid or private, and we already support that, that says we support 70% of the cloud market already. The only thing we don't support is what's called multi-tenant cloud. That's your Amazon and your Azure, where multiple users from multiple companies are calling in and being serviced by the same piece of hardware in the same application. That is an extremely complicated engineering task to be able to implement in a multi-tenant cloud.

I have one of the top cloud architects in the country, Byers Parsons working for me. Byers is working nonstop on that implementation. He believes he'll have that done by the end of the year with his team. So we are continuing that. But again, I'm not out hiring more resources trying to get it done faster because the urgency to get it done seems to be a lot less. I only have one customer to date that has a multi-tenant cloud environment that has asked me for Shield. All of the other customers that talked cloud ended up either having a private or hybrid cloud where Shield works for them today. So the majority of the market is available to the Shield product currently today.

Zachary Cummins - *B. Riley Securities, Inc., Research Division - Analyst*

Understood. That's helpful. And then just final question for me. I know not really your focus, but on your legacy government business, it sounds like you've started to see a recovery on that side. I mean, how should we be thinking about that business in the upcoming year, just given the challenges that you faced in 2020?

©2021 Refinitiv. All rights reserved. Republication or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. 'Refinitiv' and the Refinitiv logo are registered trademarks of Refinitiv and its affiliated companies.

REFINITIV

Jack B. Blount - *Intrusion Inc. - President, CEO & Director*

Well, I mean as I've always said, the legacy business is a flat business. It's been a flat business for 20 years. So I've never said there's going to be growth in the legacy business. I sustain and support and continue the legacy business primarily because I view it as my R&D center. And I know I've said this before so I mean I -- that is where Intrusion gets access to the newest, hardest, most complex cyber breaches that the government has experienced that they want outside help with, and therefore, we get to be involved in those and learn from those and be cutting-edge of the latest and greatest thing that's going on.

So we continue that, not because I think it's a growth business, because I don't think it is a growth business. It's a stick -- it's a stand-alone self-profitable business, but I view it as my R&D center. That gets me the cutting-edge cybercrime attacks out of China and Russia that I don't have to wait to see at a customer site. So we're going to continue that. We are seeing those -- that revenue dollars come back. We think we will see about the same status that we've had at about that $10 million annual revenue number that the company's basically operated at for 20 years.

It's just a niche market. So it's not -- it's just not likely to grow for -- significantly. But at the same time, it is valuable. So I am going to maintain it. I have the same people working on it, the same skills. I haven't pulled anybody off of it. I'm not -- in fact, I promoted Mike McClure to be the VP, to focus on that because the CEO, Ward Paxton, used to focus on that business, when he was here. He's not here, and I'm focused on the Shield business, so I promoted Mike to a VP so that he can full-time, focus on maintaining that business for me.

Operator

Our next question comes from the line of Ross Taylor from ARS Investments.

Porter Ross Taylor - *ARS Investment Partners, LLC - Partner*

Jack, can you walk us through a little bit there, the testing adoption process you expect from the large corporations and government agencies? You've commented that you thought they tended to be slow and kind of process-oriented in their adoption cycle. But yet, they're the ones knocking down your door, it seems, at this moment. So can you walk us through how long does it take? Should we think about it as being each of those like being a beta test? And what kind of resources do you need to commit to help get those over the line?

Jack B. Blount - *Intrusion Inc. - President, CEO & Director*

Well, sure. I'll be glad to comment on that. One, certainly, I am extremely pleased and excited by the demand that we're getting out of that segment early on. That's not normal. I think that is a direct result of the SolarWinds breach and the fact that it took out 16 federal agencies. I think they're all burning, right now, bad from this breach. They're all in panic mode, and therefore, they're willing to be a little less -- a little more aggressive in looking at new technology.

So I think it's going much faster than I thought it would, both by the level of interest and by the work they're doing. They are taking the product. They have put it into use in their environments. And the feedback there giving us is that their mouths are still open, they haven't closed yet. They are shocked every day. Every day, they're telling whoever the account person is that's working with them, that they're shocked that they can't find anything wrong with the product, that it does everything we claim it does. And that there's the volume of traffic of malware that they were never seeing before that was existing on their network anyway that they didn't know was there, that we're now identifying for them. So I think the adoption will be much faster than anticipated.

I think we will see that sales cycle happen certainly this year. Normally, if you've ever been in IT, you know that historically, since my days at IBM in the '70s, the sell cycle for IT technology was 12 to 18 months. I mean that hasn't changed literally in 40 years. And I think that's still what Gartner and Forrester will tell you the answer is today. I believe we're going to see organizations in the federal government and in Fortune 100 companies,

©2021 Refinitiv. All rights reserved. Republication or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. 'Refinitiv' and the Refinitiv logo are registered trademarks of Refinitiv and its affiliated companies.

REFINITIV

make a decision in a 6- to 9-month time frame instead of a 12- to 18-month time frame to implement the Shield product to put it in place and get that protection out of it.

So we're spending very, very little resources to support those. So again, we don't have to go on site. We don't have to put anybody on a plane. We don't have to get online for hours to configure the product. They take it out of the box. They plug it into whatever part of their network that they're willing to trust it on, and they turn it on and they start monitoring what it's doing for them, and they're not having any problems. So they're not opening errors. So basically, we get feedback of how large their kill rate number's growing every day that they didn't expect and they can't believe, and it's more out of disbelief, can this really be going on? Is it really what I'm seeing?

It's just -- to me, it's just phenomenal. I think it's going to result in positive sales much quicker than we expected. Again, nobody has reported a bug. None of my new implementations for trial products have reported a bug to us yet that we're working on. And they have not reported any failures of the product. So they're simply evaluating it. And when all you're getting is everything is thumbs up, I don't know how they don't move forward.

Porter Ross Taylor - *ARS Investment Partners, LLC - Partner*

Okay. Now do you -- would you anticipate -- you've worked with the government before, as I, and the government is not always the most efficient place to operate between cycle, between budget cycles. We're in the middle of a fiscal year. Do you anticipate any type of pushback from those people who write the checks to implementing this? Or because of SolarWinds and the like, do you think this is the type of thing that if they want it, they will get it?

Jack B. Blount - *Intrusion Inc. - President, CEO & Director*

I absolutely believe -- again, I was there for 4 years as a CIO, I watched what happened to budgets during breaches. I know what happened when I got brought in. I believe that the federal government has already made offers of money to every department for cybersecurity enhancements. In fact, they are mandating cybersecurity enhancements. I know I've been told that by multiple people. So I believe the money is available today, regardless of the time of year, the budget cycle for them to fund a new purchase of cyber -- of the Shield solution to protect their agencies.

So I don't believe that's going to be an issue at all. I don't think the transformation from Trump to Biden is going to have anything to do with it. I think any President of this country is aware and concern about the threat cybersecurity, cyber warfare brings. And I think the SolarWinds, again, this was both Russia and China involved in this. And I think it's got everybody scared that things are worse than they thought it was.

Porter Ross Taylor - *ARS Investment Partners, LLC - Partner*

I'll leave you with that. I wish you good luck with getting that first major customer in. I think that there's still a lot of people who feel that this is too good to be true. I think the market reflects that, and if we're able to get the validation of a major government contract or a major Fortune 100 or Fortune 500-type company that has a broad international reach, I think it will put the naysayers to rest.

Jack B. Blount - *Intrusion Inc. - President, CEO & Director*

It's a very quick one. I totally agree to you, Ross. I appreciate your comments. I'm going to be in D.C. in 3 weeks, again. So again, I am putting a high priority on this because of the impact it will have on businesses as well as just the overall marketplace. So it's very, very exciting.

Operator

(Operator Instructions) Your next question comes from the line of Howard Brous from Wellington Shield.

©2021 Refinitiv. All rights reserved. Republication or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. 'Refinitiv' and the Refinitiv logo are registered trademarks of Refinitiv and its affiliated companies.

REFINITIV

Howard D. Brous - *Wellington Shields & Co., LLC - Broker*

Jack, when you discuss Fortune 100 to Fortune 500 companies, can you give us a sense of the potential size of how big or how small a client could possibly be here in terms of number of seats?

Jack B. Blount - *Intrusion Inc. - President, CEO & Director*

Yes. I mean they're all big. When you talk Fortune 100 and Fortune 500, Howard, they're all big. They are, every one, big. Again, I don't want to be misleading, I don't want to, certainly -- but again, I've dealt -- most of my career, I've sold to the Fortune 500/100. I know those companies well. I know how big they are.

One of the things that's unique, I think, in the cybersecurity space is you're not likely to make a cybersecurity purchase for a segment of your business as you do in most other technologies. You're going to either believe that this is a show -- this is a game changer or it's not. And if it's a game changer, you're going to want every seat in your company on it.

So -- I mean, certainly, most of the defense contractor, Fortune 500, 100 companies that we are talking to right now are in the 100,000 seat range day 1. Any one of them makes us a rock star, and there's multiple ones that I'm in discussions with right now, all of the names you would recognize in 1 second.

Same with Fortune 100, 500 businesses. Again, one of our beta customers which became a purchaser is much bigger than I thought. I actually did not know about their international components, to tell you the truth, during the entire beta process. I thought of them as a U.S. company. They're a manufacturer here in the U.S.. I only learned when I met with the CEO, I guess it was about 6 weeks ago, 7 weeks ago, that he had subsidiaries in 8 other countries around the world and that he's already told his Board he's rolling it out internationally as soon as I can get clearance. So again, that was a complete surprise to me. They went from what I thought was 1,000 seats to potentially now 8,000 seats, and that's just a midsized U.S. business.

Well, I thank you very much for following us and I appreciate your question and I look forward when we can announce some of these customers and give you real details. It's an exciting time to be out there in the market with what we have.

Operator

And there are no further questions at this time. I'll turn the call back over to Jack Blount for some closing remarks.

Jack B. Blount - *Intrusion Inc. - President, CEO & Director*

Again, I want to thank you all very much for following the company, your involvement with the company, your advice that you've given me during individual phone calls. I do appreciate interacting with you.

This is, I think, the most exciting market right now in the world to be in. Cybercrime is growing at an exponential curve, all of it bad. And we are really the first solution to come to market with patented technology. We filed 19 different patents. We don't know how many of those we'll get, but we know that we'll get many of them so we can defend this technology. We know that our TraceCop database is a one-of-a-kind database. There's nobody else sitting around with another database that they can point their AI at and have it get as smart as our AI. There simply isn't a second database in existence, and that's why our database results are 5 9s of accuracy as compared to 30% error rate of everybody else's product.

So thank you very much for working with us. Thank you for your patience. I appreciate your excitement. I know you all want to hear me announce new customers, but it does take a few weeks and a few months to sign up big companies and move the needle like this. It is going to be a very, very exciting year. Trust me.

©2021 Refinitiv. All rights reserved. Republication or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. 'Refinitiv' and the Refinitiv logo are registered trademarks of Refinitiv and its affiliated companies.

REFINITIV

Thank you again. Have a great evening.

Operator

Ladies and gentlemen, this concludes today's conference call. Thank you for participating. You may now disconnect.

DISCLAIMER

Refinitiv reserves the right to make changes to documents, content, or other information on this web site without obligation to notify any person of such changes.

In the conference calls upon which Event Transcripts are based, companies may make projections or other forward-looking statements regarding a variety of items. Such forward-looking statements are based upon current expectations and involve risks and uncertainties. Actual results may differ materially from those stated in any forward-looking statement based on a number of important factors and risks, which are more specifically identified in the companies' most recent SEC filings. Although the companies may indicate and believe that the assumptions underlying the forward-looking statements are reasonable, any of the assumptions could prove inaccurate or incorrect and, therefore, there can be no assurance that the results contemplated in the forward-looking statements will be realized.

THE INFORMATION CONTAINED IN EVENT TRANSCRIPTS IS A TEXTUAL REPRESENTATION OF THE APPLICABLE COMPANY'S CONFERENCE CALL AND WHILE EFFORTS ARE MADE TO PROVIDE AN ACCURATE TRANSCRIPTION, THERE MAY BE MATERIAL ERRORS, OMISSIONS, OR INACCURACIES IN THE REPORTING OF THE SUBSTANCE OF THE CONFERENCE CALLS. IN NO WAY DOES REFINITIV OR THE APPLICABLE COMPANY ASSUME ANY RESPONSIBILITY FOR ANY INVESTMENT OR OTHER DECISIONS MADE BASED UPON THE INFORMATION PROVIDED ON THIS WEB SITE OR IN ANY EVENT TRANSCRIPT. USERS ARE ADVISED TO REVIEW THE APPLICABLE COMPANY'S CONFERENCE CALL ITSELF AND THE APPLICABLE COMPANY'S SEC FILINGS BEFORE MAKING ANY INVESTMENT OR OTHER DECISIONS.

©2021, Refinitiv. All Rights Reserved.

©2021 Refinitiv. All rights reserved. Republication or redistribution of Refinitiv content, including by framing or similar means, is prohibited without the prior written consent of Refinitiv. 'Refinitiv' and the Refinitiv logo are registered trademarks of Refinitiv and its affiliated companies.

REFINITIV