REFINITIV STREETEVENTS

EDITED TRANSCRIPT

INTZ.OQ - Q1 2021 Intrusion Inc Earnings Call

EVENT DATE/TIME: MAY 04, 2021 / 9:00PM 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

B. Franklin Byrd *Intrusion Inc. - CFO*

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

Joel Achramowicz *Shelton Group - Managing Director*

CONFERENCE CALL PARTICIPANTS

George Russell Cleveland *RENN Capital Group, Inc. - President & Sole Director*

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

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

Scott Christian Buck *H.C. Wainwright & Co, LLC, Research Division - Research Analyst*

Jay Bruno *- Private Investor*

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

PRESENTATION

Operator

Good afternoon and welcome to INTRUSION's First Quarter 2021 Results Financial Conference Call. At this time all participants are in a listen-only mode. At the conclusion of today's conference call, instructions will be given for the question-and-answer session. 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 Achramowicz *- Shelton Group - Managing Director*

Good afternoon and welcome to INTRUSION'S first quarter 2021 earnings conference call. I am 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 CFO.

Now 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. 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 2020 Form 10-K filed with the SEC on March 9, 2021, and other SEC filings made from time to 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 today, Tuesday, May 4, 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.

Now we'll 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 be happy to take your questions.

With that I'd like to turn the call over now to INTRUSION's CFO, Franklin Byrd. 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

B. Franklin Byrd - *Intrusion Inc. - CFO*

Well, thanks, Joel, and thanks to everyone who has joined us today. So for the first quarter 2021 revenue was $1.9 million compared to $1.6 million in the fourth quarter of 2020, and $1.8 million in the first quarter of 2020. Revenue for the first quarter continued to reflect the impact of extended government shutdowns related to the pandemic, but we're hoping to see positive signs of recovery as Washington begins to reopen and more normal ordering patterns return throughout the course of the year. Gross margin in the first quarter was 66% compared with 58% last year, and 58% in the first quarter of 2020. First quarter operating expenses were $5.1 million compared to $4.8 million last quarter, which included a $1.1 million non-cash write-off related to a prior office lease arrangement. This compares to operating expenses of $1.5 million in the same quarter a year ago.

As mentioned in the last quarter, the increase of operating expenses is due to the additional hiring we've had to expand our sales and leadership team combined with increased marketing focus on the development and launch of Shield. To drill down a little further on the additional employees, since the first quarter of last year, 2020, the company has hired 38 additional employees across the board for the development and launch of Shield. The breakdown of these new employees were as follows; 26 in sales and marketing; 8 in research and development; and 4 in general and administrative areas. In addition to the newly hired employees, we've also increased our use of contract consultants for both research and development and our legacy consulting business. As I previously stated, we have continued to step up our marketing efforts in 2021 focusing on the launch of Shield. Additionally, we've experienced general expense increases which you would normally expect from employee headcount increases.

Net loss for the first quarter of 2021 was $3.9 million or a minus $0.22 per share on 17.6 million weighted average shares compared to a net loss of the same $3.9 million or minus $0.23 per share in the prior quarter and a net loss of $0.5 million or minus $0.04 per share in the first quarter of 2020. Cash and cash equivalents as of March 31, 2021 were $13.1 million compared to $16.7 million in the prior quarter and working capital was $12.4 million and total outstanding debt at the end of the quarter was $635,000, including the current portion.

In terms of guidance, we will continue to keep with (added by company after the call) our current policy of not providing quarterly guidance at this time, due to the fact that we are still in the early stages of ramping orders on Shield. As we've stated previously, it's very difficult at this stage to accurately predict the exact nature and timing of the revenue ramp but we'll continue to reevaluate this on the quarters ahead.

With that, I'm pleased to pass the call over to Jack to review recent business developments with Shield and several other activities across the company. Jack?

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

Thank you, Franklin. So I'm going to start off by certainly commenting on, I think the excellent progress that we made in first quarter because I'm certainly very pleased by it and think it's a good indication of the direction we're headed. We've had an actual unprecedented interest in a very short period of time in the Shield product, it's unique functionality and it's unique plug-and-play technology that makes it so easy to implement and evaluate. We have struck a number of contracts, most of those being 3-year contracts with some significant companies, 2 of those for example Kimberly-Clark, which we did a press release on and LCI, which we did press release on. Kimberly-Clark's a Fortune 500 business, LCI, I believe is a Fortune 2000 business, both of them are international businesses with international locations, and they have signed international agreements for 3 years to be able to use the Shield product in all of their international locations. So that's very, very significant in the first quarter of a new launch of a new networking technology cybersecurity product. We're very, very pleased to have both companies on board. We are working very closely with both companies and very excited by the progress that we're seeing there. Having well-known brands like this certainly increases the opportunities with other companies to make additional new sales. In total, we have licensed over 50,000 seats to date with these companies. That's an extraordinary success I think in a very short period of time.

Our pipeline continues to grow with prospects from the SMB market, from the mid-market and certainly from large enterprise and even government agencies. I was in D.C. all last week for example, and was very encouraged to see the streets full of cars, hotels full of patrons and business coming back to normal in the federal government. As you know I reported last year when I was up there and found it to be very depressing place. So I was very encouraged to see business coming back to normal in the capital.

©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 have been performing multiple demonstrations on the Shield technology, which is very easy to demonstrate to a customer through a web session online every day of the week. We continue to have very positive feedback from those and very positive outlook for the year. Revenues, of course, will grow slowly because of the SaaS model of our technology, it takes a while for that to ramp up.

So from an update from the sales channel, we have 35 resellers now actively selling our product for us and I'm proud to say, some of those already are international resellers. We have 3 Canadian resellers, 1 Mexican reseller, 1 United Kingdom reseller, 1 Australian reseller and actually 1 Lebanon reseller. So 7 international resellers signed up in the last 4 weeks along and we're very excited about that, because I believe the international market is very, very ripe for new cybersecurity technology.

If you look at the international market, for example, some people may be surprised, but the 4 leading countries I think that you see are Mexico, Brazil, I just drew a blank on the other two. But anyway, not necessarily normal where you'd think of them coming from. Brazil and Mexico being the two largest outside of the U.S. for cybercrime, aggressive attacks and hits on a daily basis. So, we're excited to have international resellers signing up as well. We've expanded our leadership team by adding 2 key individuals to the team very, very recently. We originally had not planned to hire a Chief Sales Officer until 2021, because we originally thought it would take until 2021, I mean 2022, to become international. We got that done by the end of first quarter and with that change, we went ahead and made the move to hire an international Chief Sales Officer with tremendous international experience, established known resellers in businesses that he is used to working with. In addition, he brought on a new VP of Direct sales, Jeremy Merrick, so Darryl Athans and Jeremy Merrick, our two new executives in sales. We're very excited to have them both on the team. We had them here in Dallas recently for training and they're out actively selling the customers today.

On the traditional government business, we are seeing early signs of growth, although there are still delays due to things that are going on in the government. For example, while I know we all hear daily on the news about the President talking about massive spending increases, sadly, we do not have an approved budget for the government, and it's not looking like the budget is going to get approved until 2022. Without an approved budget, then the government must pass continuing resolutions, which we've seen before in the past.

The challenge with continuing resolutions is starting up new business. So ongoing projects can continue to be funded, but new projects are very hard to get approved and funded during continuing resolutions, so that may still cause some delay as we move into 2021. However, we expect to see near normal growth continue closer to the end of the year.

In summary, Shield is an early stage of ramping and we're very excited about how it looks. Our pipeline is extremely large for the early stage of the company. It is significantly larger than I would say it needs to be, to accomplish the goals in sales that we expect for 2021. So, I believe we have a great pipeline in front of us that we're executing against, clearly will be driven to accomplish, implement new sales, which bring on new revenues. Our target for international is also an exciting change that we do not think we would have at this time. Again, Brazil, India and Mexico being the three largest countries for the international market that are prime for our ready growth. We have established resellers that we're talking with that we'll be bringing on in Brazil and India very shortly. We've already brought on Mexican reseller and have others in the pipeline as well. So we're continuing to build market visibility for Shield, it's unique capability of real-time killing all dangerous traffic incoming and outgoing to your network.

Fundamentally, I'd say the two questions I get asked most frequently when I'm doing sales pitch is, why is Shield producing such dramatic higher kill rates than any other cybersecurity product on the market? And the answer I gave to that is, Shield has the advantage of using the TraceCopTM database that we've had for 25 years, that's the largest and the most unique in the world to train our AI. So therefore, our AI can be dramatically more enhanced and more significant. On average we're showing about 20x the volume of traffic that we are identifying is dangerous to your company compared to other cybersecurity products. So not only do we not generate any alerts that waste hundreds of hours of man-hours by IT teams tracing them down, we are killing thousands more things than other products even identify and generate alerts on. So the community is starting to readily adapt to Shield's nature of understanding the broad, breadth of the cybersecurity brush that is sweeping across the world, that's impacting business, with an attack reportedly every 39 seconds on the business.

With that, I would like to turn it over and open it up to your questions. And as always, we will do our best to answer all your questions. Operator, if you could open the call up.

©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

QUESTIONS AND ANSWERS

Operator

(Operator Instructions) Our first question comes from Zack Cummins of B. Riley Securities.

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

I just wanted to start off by asking, if you could just give us a general sense of kind of the company of the contribution of the legacy business versus maybe the kind of normal (corrected by company after the call) Shield revenue that you're able to get in this quarter. You saw a nice tick up in the gross margin line versus maybe what we saw over Q4 and Q1 of last year.

B. Franklin Byrd - *Intrusion Inc. - CFO*

Zach, this is Franklin. Yes, so in Q1, virtually the majority of all of our revenue came from the legacy products. We had, as we expected and have always communicated, our Shield sales in Q1 was very minimal because we just launched in Q1 so. But what you see for Q1 revenues is largely and predominantly the legacy business.

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

Understood. And then, understand I guess I don't want you to provide guidance just given how early you are in the stage of this. But is there any way you can give us a sense of the number of Shield seats that you have right now that are paying versus what you just signed up in the backlog?

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

Well, we don't have the exact number of those that are paying today versus our signed under contract. So, the 50,000 seats are under contract for Shield but they -- because of the SaaS license, they only pay revenue online in a quarter. So initially, if you have 20,000 seats, you do not turn around 20,000 seats in one quarter, because you have to have IT people alert, they have to know what's going on. Again, Kimberly-Clark for example actually has locations in 110 different countries and they're planning to roll out worldwide. So, we have not seen their implementation schedule of how they're going to get 110 countries, but we know that they're working on it. So, the revenues will come in as they bring on a territory or region and then the revenue start paying. So, the SaaS model is you pay as you use. So, as they ramp up and implement across the market, then we'll see more and more seats. So, the 50,000 seats is what's licensed, but it's not what's being paid for daily.

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

Understood. And then you kind of touched on this, but with that 50,000 seat backlog, I mean, what sort of the pace that we should anticipate for that rollout for these to go live? I know it can kind of vary customer-by-customer, but I'm just curious how you're thinking about it internally as you build out your plan and your model moving forward?

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

Well, again, I don't -- we don't have enough track record to have history to understand how fast customers are going to be able to implement. We've done everything humanly possible to make the product, the easiest product to install and implement ever invented. Again it's -- most customers, in fact, we had 1 customer that I travelled to New Orleans to sell a few weeks ago and their concern and fear was from their IT department and not having the resources to take time to learn a new product and implement it. I literally showed up at the meeting, walked into the datacenter with the CEO and his entire team, installed the Shield product and had it active in 3 minutes timed on the stopwatch. It was in production in use. So we've done everything humanly possible, but how fast customers rollout products is all about their customers. So, they don't have to give us a

©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

plan of when they're rolling out which ones, we know when they come online and that's when they start paying for them. So, I would anticipate that they'll bring on some number of seats each month, but I don't know at what rate and we don't look at history to look back and say. They could turn it all on in 3 weeks, they could turn it all on literally in a day, if they wanted to. But most companies don't operate that way, they go by location, they roll things out in a physical location one at a time. They probably will roll up an entire location, which could easily be 1,000 seats coming on at once, it could be 300 seats. We just really don't have any data, Zach, to be able to determine that. We don't control it, the customer controls it. So I'd like to give you answers, but I just don't have enough data, I would be truly guessing and I don't know that.

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

Understood. And then I guess, just final question for me. In terms of Kimberly-Clark, I mean how that contract is structured? I mean just depending on the number of seats. Are their requirements where they have to fill those seats over a certain time frame? I'm just curious if it just gives them the option to make a certain number of seats go live or are there some sort of contractual obligation that requires them to roll this out and actually begin to pay for it?

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

Certainly there is the intent and the desire that Kimberly-Clark will be rolled out fully within 12 months from the very first discussions I had with them. I have not seen a schedule and there is not technically anything in our contract that requires them to implement it in a certain time frame. So I know they have some seats implemented already. In fact, they have some seats implemented at the time of the press release. I know they're rolling out more aggressively, but I haven't seen their schedule. So I certainly anticipate that they will have all of their seats online within 12 months. I would expect probably more like 6 months, but again, I don't have the history to prove that. I mean clearly, they didn't buy this to sit on the shelf. They buy this because they're scared to death of cybercrime and it's only helping you if you get it implemented. So they have every desire to implement it. It's not a, I don't want to spend the money, because it's very inexpensive versus what they are paying for other products and the risk they have if they get hit. So I know they plan to be very aggressive with rolling it out, and I think most customers will be.

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

Understood. And then I guess just a final question from me would be, around kind of all the hiring that you've done over the past couple of quarters. Do you feel like you really have kind of the team in place right now for the expected demand for Shield or how should we think about the ramp with operating expenses over the next couple of quarters?

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

No, we have said, I think a couple of times that, we think that we have filled the critical positions we have in the company, the sales force, the technical support people, the quality assurance people, all the things that go along with shipping the production product. So we feel like our headcount is largely stable right now. I'm sure we'll be hiring 2 or 3 people a month or a quarter, but we don't have any aggressive hiring plans until we see what the implementation ramp is and where additional people are needed. So as we said before, we think we're pretty stable at about the headcount we are right now to get us through second quarter. We'll evaluate -- right now, we have plans for a Board Meeting right around the end of second quarter to evaluate with the Board what we've accomplished in sales and revenues and whether it's time to re-engage in new hires or whether we're going to stay stable for another quarter. So it will be evaluated each quarter.

Operator

Our next question comes from Scott Buck of H.C. Wainwright.

©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

Scott Christian Buck - *H.C. Wainwright & Co, LLC, Research Division - Research Analyst*

First one from me, kind of piggybacking on Zach's question. Outside of personnel is there any other investment you need to make to feel like you have the infrastructure in place to properly roll this out?

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

No, we have no major infrastructure enhancements planned. Our data center is stable in place and at adequate capacity, so we don't have any anticipated expense that will drive anything new right now.

Scott Christian Buck - *H.C. Wainwright & Co, LLC, Research Division - Research Analyst*

Can I get one. Can you remind us the difference in economics between selling directly through your sales force and using the reseller channel?

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

Well to the reseller channel makes 30% off of our product, which is basically how most of these evaluate internal cost of direct sales versus channel sales. So while one may sound more expensive and more profitable than the other one, both of them basically cost you about 30% to close sales, whether you are doing it through a direct sales force or whether you're doing it through a channel sales force. So that's pretty much an industry average number, that's how we get to it and that's how they compare.

Operator

Our next question comes from Ross Taylor of ARS Investment Partners.

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

Jack, on the last call you talked about a number of large and potentially very large prospects, that you said you were in the demo stage or trialing stage. Could you update us on where those potential customer stand?

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

Well, certainly LCI and Kimberly-Clark were two of those. Again both of those are very large companies. As I said I think LCI is in the Fortune 2000 category. I know Kimberly-Clark is in the Fortune 500, I think they are Fortune 330 or something. So those are certainly two of the companies that had early access to the product, got early evaluations, that I was alluding to during that call. Kimberly-Clark being certainly I mean, we talked about a lot but to win a Fortune 500 company at this early stage of a new technology is almost beyond my excitement. The work that they put in to evaluate technology, the impact it has on their company, again looking at rolling it out in a 110 different countries. I mean this is a major, major enterprise decision and they don't make those lightly. So we feel like this is as good of a rubber stamp as you can get that says certified, ready for production. So we're very proud of that. There are others in the works and it was not just 2, these moved the fastest. Fortune 500, Fortune 100 companies, government agencies generally take 9 to 12 months to make a decision on a new networking technology, I mean, pretty much anybody in the industry will tell you that. I've been selling enterprise solutions for 42 years, so I can tell you, it's always. In fact, in the earlier days that we used to say, it was 12 to 18 months now say 9 to 12 months. So some of these big companies will take longer, both to make the decision to put it in evaluation mode, how long they want to evaluate it. But we are in discussions with other Fortune 100, Fortune 500 and government entities that are very large and very significant, that we're very excited about and that I will continue with my team to work closely on.

©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

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

With regard to the government agencies, are they seeing this as something that they would be putting into place in replacement of services you currently sell them or would this be additional and for different uses than the work you're currently been or the historical work you've done with them?

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

No, it's absolutely new and additional work. So this is really, again, I think I said earlier in the call, I was in D.C. all last week, specifically to work with government agencies. Was really my first time that I've been able to go up there and meet with them and give them demos of Shield and talk about the new functionality and how it works and how -- I think it's -- so, again formerly be in a CIO in the federal government, I know a lot about what their needs are, and so I know a lot about how to sell to them. So this is additional, they will not displace any of the current work that we do for them, but it's an additional as they would be rolling out to large agencies to all of their employees and their organizations to protect them. So I got an incredibly warm reception all last week in D.C. The demos were well-received by the government as they have been by any company I have shown. We have follow-up meetings with every one of these agencies in the coming weeks and months. So I'm again extremely excited about how rapidly, how openly they accepted the Shield technology. They absolutely love the concept of killing things rather than generating the reports. They all have their own military analogies to the fact that being protected instead of reporting that you have been hurt after the fact was a radical departure and something that they saw endless value add up.

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

Okay. And so, looking at all of this and you made the comment that Kimberly-Clark was by you seen as effectively a proof-of-concept that, the market there's a lot of uncertainty clearly, the recent price action in the stock market has indicated that there are lot of people who don't have the confidence in this product that you have and that your team has. So can you comment on why this proof-of-concept was so important? Because obviously in the market -- we've have seen a lot of action that indicates that people don't believe that it means anything.

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

Well, I wouldn't agree with that statement. I think everybody knows they need better cybersecurity. I think everybody feels vulnerable, every article I read, every conference I go to, I never hear anybody say they don't need anything. Now not having the confidence in INTRUSION Shield, given the fact that it's such a new product out of a new company in the sense that we're a turnaround, because we've never had a commercial product, I certainly understand their hesitancy on that front and I think it's normal. But again, traditionally, if you buy like a firewall, you're going to spend weeks to months configuring it, then you're going to put it on your network, and then you guys spend months evaluating, did it really help me and how is it better and how do I know it's better. So these are traditionally solutions that take long periods of time to evaluate. Shield on the other hand installs in 2 to 3 minutes and start to work on the network immediately. Most of the time when I do a demo, we kill from 10 to 20 to 30 malware attacks during a 15 or 20 or 30-minute demo to the customer. So they real-time can see the benefit of this product. Again, if they typically run a month-long evaluation, they're going to find that we killed over a million connections on their network that they didn't even know were going on, that weren't useful, that weren't helping their employees, they weren't constructive, that could only have bad intentions, that none of their other products were even generating alerts on. So, the value of Shield is so dramatic that I believe the market is going to adapt it very, very quickly. And I think that's why I'm so excited about a company of the stature and size and speed generally, lack of speed of a Fortune 100 company to move, step forward and step up to the plate and say, we want this protection in all of our locations around the world. I think that really proves what I'm excited about and when I think every customer sees when I demo the product.

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

Can you give us a little bit more color about your database and what makes it so unique? I know that there have been indications and some people in the market, they have indicated that they believe it's just off the shelf data. Our efforts indicated to us that it's actually almost, what I would call forensic data not being a technical specialists. But can you go into more of your database and why no one else has that capability?

©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*

Sure. So you have to attribute this back to Ward Paxton, PhD that founded this company 37 years ago. Launched several unique products in several markets, fiber optics, firewalls, et cetera. He is a brilliant man. When the Internet launched, he envisioned the fact that tracking Internet traffic would be the forensics that you need to really know what's going on in the world. So he set up and started a database 25 years ago, to track international traffic connections from all points A to B around the world, on the Internet, real-time, the forensics, who's talking to what, what kind of data are they sending, what is their IP address, what is their URL et cetera, et cetera, et cetera. So they started tracking this information. And for a long time, I don't think they really had a plan of what they were tracking it for, but except that Ward had of vision that data would become valuable. Well, after a few years and they started getting all these government contracts to do forensics work, they found that the only way they could solve these problems the government was bringing was to do research in this TraceCop database that they had been building that nobody else in the world had because nobody realized that tracking information is important. So we spent the last 20, 25 years doing forensic work for the DoD on cyber breaches that they can't figure out on their own, that's why they hire us as consultants to engineer and figure them out, and the only way we can figure them out is by using the TraceCop database, and so much of that is actually done based on historical relationships and connections. So, while you may think, something that happened 15 years ago on the Internet, isn't relevant, our research shows that about 70% of the time that we determined something to be evil or malware in nature, it's based on historical information that's in the TraceCop database, because all of these sites are constantly changing their IP addresses, they're constantly changing their URLs, they're constantly trying to disguise themselves as innocent and new and safe and clean. And it's only to have that is historical information that you can trace back and so, this is really China Joe doing his evil thing again. So, the reason that our database is so valuable is because 1) it's huge, it's petabytes upon petabytes of data; 2) it's 25 years of all connectivity history on the Internet. I do not believe another database exists in the world like it. I -- when I was in the government as a CIO, I put a bid out to buy a database that had more than 10 years of history and no vendor could provide me such a database, so they never could collect on the money. So, I believe this database is truly unique. Again, you have to understand how AI works to understand why that's so valuable, and most people really don't understand AI much at all. If you give AI a small amount of data, it's going to either tell you nothing, it's going to tell you something wrong. AI can only learn out of massive amounts of data. So, I worked on a project to solve diabetic blindness, for example, a few years back. The doctors from all over the world that were involved in that project didn't have a clue what caused diabetic blindness, but we had data from hospitals all around the world. Then we created a massive data-like and then we had so many AI algorithms that looked at the data and the data came back and said, this is what causes diabetic blindness. 30 years of your research couldn't figure it out, a few weeks of research with AI came back and said, this is what causes it and this is how to cure it. America now says diabetic blindness is 98% cured, that's because you have to have the massive history of data. Look at Tesla car, go talk to anybody with Tesla, about how that your Tesla car can make a decision of whether to change lanes or whether to turn or whether to -- how does -- how to drive -- how you have driverless taxis in Phoenix right now. I just rode one a few weeks ago. It's a little bit scary but a driverless taxi has to make millions of decisions every second of the day and it does that off of studying historical data about driving patterns. So, that's why the TraceCop database is so incredible. You look at the rest of the world, they will tell you there's about 500,000 known malware active sites on the Internet today. When we pointed our AI at the TraceCop database, we thought like everybody else, there is 500,000 of them. Well, the AI came back and said, there is 3.4 billion active malware sites on the Internet today, that's 1/3 of all Internet connections and it can tell you the IP address of every one of them. So we're not just protecting you from 500,000 signatures, we're protecting you from 3.4 billion bad actors every second of every day. We could only know that. There is no way to know that. There's nobody on the planet that can prove that number because nobody else has our database. But that's a documented database of dangerous identified IP addresses. That's what makes Shield so different, that's why our TraceCop database is so proprietary and valuable to this company. Does that answer it?

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

Yes, I think it actually does. I'm going to leave you with one last -- it's not a question but it's a request. By our calculations that when you get to kind of full run we expect each 50,000 seats you generate is probably worth about 4$ or $5 a share in value. I don't need you to come out and tell me every time you win a big contract, but what I'd love is, in these early days to show to the market that you're getting traction, that you will let us know at various important benchmarks. Said we like when you talked about being over 50,000 seats, when you get 100,000 seats, you can let us know when you get 150 to 200. Because it seems to me right now that this is something, I've learned long ago is that, I don't necessarily have to know how a product works, but I know that if the right people and if smart people are buying it and using it, then it probably does work, and it seems to me that right now the proof-of-concept here is really going to be showing the market that there are people out there who actually know

©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

more than they do about these issues, that are making the choice to use this product. And as I said, the leverage by our model is huge. And I would welcome that kind of information as affirmation.

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

Thank you for that comment. I agree with it completely. We will absolutely keep the market appraised of our seat count as it grows. As I've said, we won't be able to do every product, I mean, every release to every customer, because a lot of them won't allow it, but again, we had 2 large ones which were huge. We certainly can give you a seat count even if we can't give you customer names, and I think to let the market know every time we add another 50,000 seats is a very reasonable thing and we will be delighted to do that. I'm going to be excited as you are to watch that number grow because again that proves the value that we bring into the market, to help stop the horrendous cybercrime problem the world is facing.

Operator

Our next question comes from Howard Brous of Wellington Shields.

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

Jack, in several past calls, you talked about that Shield prevented SolarWinds, can you describe how that's possible? On how you refine that up? Please go ahead.

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

So, you have to understand how Shield works a little bit. So unlike most cybersecurity products, we don't use signatures. So let's back up a little bit. SolarWinds was what's called a zero-day attacks. What that really means is, it's a new attack with an unknown signature, so therefore no cybersecurity product can identify it and stop it and therefore it's going to breach networks until somebody identifies it and starts knowing how to look for it. That's what zero-day attack means. So when the SolarWinds attack was being launched, it was an unknown thing, so therefore, it appeared as harmless to everybody's network security and therefore it got on a lot of networks. The way we work is we identify even zero-day attacks by using artificial intelligence, this massive TraceCop database to understand patterns related to traffic that suggest its malware even without knowing what it is. So how do we identify and kill SolarWinds? Because of our AI, we identified the patterns of these attacks and said, this looks like evil stuff to us, we're going to kill it not let it happen. But we write that in our database. So, at the time we were doing this last August, September, we didn't know that was SolarWinds, because SolarWinds hadn't been identified yet. But we were seeing things we thought were evil that we were killing. Well, once SolarWinds became public, they identified the signatures, they published them on the Internet and everybody could go start looking for them on their network and trying to clean it off their network. We went back and looked in our database and said, yes, we were killing those attacks back in June, September, August before anybody knew what they were. So we didn't know that we were killing SolarWinds, but we knew we were killing new unknown attacks. That's how we start (technical difficulty) exchange attack recently after SolarWinds. Again, we were killing that attack when it came in as a zero-day attack because our AI can identify the patterns to say, this is not good therefore, we're going to kill it, because it's not good, killing it didn't hurt anybody because nobody knew it had ever been killed. And it's in our database, we didn't know it was the Microsoft Exchange thing because you didn't know what the Microsoft Exchange thing was last year. But in March, once we became public what it was, we could look at our database and say yes, we killed thousands of times the Microsoft Exchange attack, the SolarWinds attack. So that's how we can kill even zero-day attacks before anybody knows what they are and we can prove we did it because it's recorded in our database, the time and date and the number of times, and the occurrences that it was attacking. Does that make sense?

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

Makes a lot of sense. So we're continuing -- no, makes absolute sense. For years INTRUSION with TraceCop and SavantTM has been a sole source supplier to the Department of Defense. You've indicated on this call and others that, business through -- legacy business is getting better. And I

©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

want to address certainly, the one that (added by company after the call) Department of Defense and the Department of Agriculture did go through, talk with me about the opportunity there; 1, in terms of number of seats and where you stand in terms of testing?

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

Well yes, I was busy with organizations in the DoD and I was visiting with organizations in USDA, I was visiting with organizations and treasury. I was visiting with a number of organizations in the United States government last week. I was very busy. Again it was good to see the government back to work, trust me. The reception I had was fabulous. So, it was incredibly positive. A lot of questions, a lot of doubt and uncertainty, because what we do is radically different to what other products do, but I believe that they are more aware than ever that they are exposed and vulnerable and that the products they have aren't working. SolarWinds and the Exchange breach, just to name two of them that the public was aware of, proved to the federal government that they are not secure. Both of those attacks breached multiple government agencies and hundreds of thousands of employees. So they're very upset about it. President Biden just announced that he is working on a new bill to dramatically change the requirements on the federal government for their cybersecurity defenses because he believes what they've been doing is inadequate. We met with people who are aware of that bill, that we want to make them aware of what Shield is, how it would make the government safe and we are trying to constantly get more exposure in the federal government to understand how Shield works and how we can help them solve their problems. So the government is very, very serious and aware of cybercrime threat and that they are not doing enough to stop it and that current cybersecurity products are not protecting them. So we believe that creates an absolutely garden opportunity for Shield to come in as a unique patented AI technology that can add a new level of safety to their network. USDA has 110,000 seats to know when you asked about seats. Since I used to be their CIO, I can answer that question. They have hundreds of thousands of seats, it's a pretty big implementation.

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

You said that -- talked about public aware on specifically SolarWinds and Microsoft Exchange. Are there others that the public is not aware of that you can comment on?

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

Well, there are certainly others that I could comment on, if I had the list in front of me, and there are major breaches announced every day. I get reports -- and it's different countries get hit with different breaches at different times. I get reports from around the world right now. I have a lady in India that's working on that part of the world and gives me reports every day. So there are breaches every day. We're going to add a section to our website very soon, where we kind of are the centralized site for learning about more breaches readily and we're going to be promoting that very heavily. I can tell you that I talked with government agencies because I do have top secret security clearance, when I was in D.C last week, about other breaches that have occurred that I can't tell you about on this call. So there are more than just the SolarWinds and Exchange that has hit government agencies in the past few months alone. Again, the government is very seriously concerned. When the President starts talking about a bill specifically for cybercrime, I think it tells you how alarmed the federal government is right now.

Operator

Our next question comes from Russell Cleveland of RENN Capital.

George Russell Cleveland - *RENN Capital Group, Inc. - President & Sole Director*

My question is around the Beta testing, it seemed like that our plug-in service, it doesn't take months of testing. So can you tell me more about the Beta testing and again, the characteristics of the companies. You mentioned earlier that there were companies similar to Kimberly-Clark and that kind of size and of course the government is very exciting. But tell me about the test they have to do here and the timing on all this. Any thoughts there?

©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*

Certainly. Well, just to be clear, terminology varies. Beta means to me and generally to the industry, a pre-release product. So our Beta testing was only being done prior to Shield going into launch in general production. Now we do evaluation systems, so they are not technically Beta systems. But it sounds like you're really talking about evaluation systems. So we are keeping evaluations out every week to various customers of various sizes. Again, the product is remarkable. One of the things I'm normally most proud of because of all the pain and agony I've had as an IT professional in the industry for 40 years, learning and installing new security products on networks is a horrible, horrible task. And so, when I helped the team here design Shield, I told them this had to be a revolutionary plug-and-play product because IT is already overwhelmed, they don't have the time to evaluate technology. So we have patented the process of how we do plug-and-play on such complex software. There is normally 100s of parameters you have to set in the network type appliance to even get it to become active. Shield plugs in, identifies its network and begins protecting you 2 minutes after you turn it on. So we can do very rapid implementations and evaluation. One example, probably the best I have so far is the one I mentioned. I flew to New Orleans to meet with the company, where I was friends with the CEO but his IT staff did not believe they needed Shield, they thought they had the bases covered, they didn't need yet another layer of cybersecurity and they didn't have the time and they didn't want to evaluate it. But he was worried enough about ransomware and breaches of other companies like his that he invited me out, to try and convince his IT department. We had a meeting in a conference room with all of these IT professionals and the CEO of the company, we installed Shield, It took 3 minutes, we turned it on and we sat there as a group in the meeting watching Shield kill things that were living on his network that he didn't know were there. They bought the product the same day. It's in production at their company now. IT, they had a loaner, I told them it's an evaluation product, I came down, when I got ready to leave, I kind of jokingly said, you know, I can take the system back with me, we don't have to leave it if you don't want to do an evaluation. And the CIO looked at me and said, you're never getting that appliance out of my network. He said I'll sign the contract today. So that's how fast it can go, typically what I'm saying is about 30 days. So not the 6 to 9 months of companies with traditional products, but about 30 days, they want to put the product on their network, they want to evaluate it and when they -- it seems like most of them call me after they get into that first 30-day report. So Shield prints out a report at the end of 30 days, telling you how many connections get killed to keep your network safe and that number is typically over a million connections in 1 month. At that point, no CFOs have taken our product off. So, in a month they know it hasn't interfered with any of the work their employees were doing. So, it's not killing things that they need, not slowing them down, they don't even see it happening. Well, it is killing a million things and that tells them there's a million things that were on their network that could only have evil intention. Something does not move on your network because it doesn't have any place else to live, it's there for a reason. It's there to find a way to hurt you. So it's very, very compelling. Hopefully, a prospect can go to becoming a customer because of how quickly Shield proves its value to a customer. Does that answer your question?

George Russell Cleveland - *RENN Capital Group, Inc. - President & Sole Director*

Yes. So the challenge here is not so much of time because it's proven very quickly, it is just legal and Board approvals and corporate bureaucracy, not testing and getting the product into the market.

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

You're right. I would say we spend more time upfront with the CFO or the CIO around administrative and legal things than we do around actually evaluating the product. The product proves itself almost automatically.

Operator

Our next question comes from Jay Bruno, a Private Investor.

Jay Bruno - - *Private Investor*

My history with your company goes back to, I believe it was 1995, possibly '96. Long time ago, I discovered the company while doing research and as far as technical research. And then I learned about the technology and it kind of had me hooked, I ended up investing quite a bit of my clients'

©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

portfolios into ODSI and I had very good relationships with -- at the time with Ward and Joe Head, the Investor Relations, man, I think his name was Gordon. Anyway, finally, something that I heard 25 years ago from Ward directly when he told me he was building a database, I just heard the results of it. 25 years later, and I'm looking at after-market trading and the markets is just a wonderful place, the way it does that. They look at numbers and they don't look at the future. Anyway, I'm a new investor in INTZ and anyway, I just wanted to kind of affirm the fact that, things I heard 25 years ago now have a 25-year track record, especially at TraceCop. I believe that was called ProtoCop in the beginning and -- yes, and I mean I was there -- go ahead.

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

I wasn't here that long so I can't attest to that only you can. Joe Head and I mentioned was Ward, Founder. Joe Head is still here, Senior Vice President in the company, he is my most valued ally and resource in the company. His knowledge on cybercrime and forensics activity is some of the top in the world. And Joe is just a pleasure to work with. I've enjoyed him ever since the first time I met him here, and certainly, he is the person that can talk to and attest to why he and Ward started the TraceCop database and how valuable he's watched it grow to be over the past 25 years. So, thank you so much for that very kind comment. That was very kind of you.

Jay Bruno - - *Private Investor*

One other thing, I just want people listening to understand, I believe this company is one of the, if not the pioneer in cybersecurity; you were looking at hackers back before they hackers. Back before there was a cybersecurity law and I believe this company had something to do with that law being going into effect. And I'm sure Joe has a lot of interesting stories. So...

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

Joe does. This company has been a pioneer in cybersecurity forensics work for 25 years. There's no doubt about it. I heard first hand from a couple of very senior, in fact one of the guys, he's is retiring next month, he knows Joe back when Joe first called on him 25 years ago and he was commenting on the amazing things that INTRUSION has done for them over the years. So, they believe that we are a pioneer and they certainly believe and we're excited in the new INTRUSION Shield product as a revolutionary game changer and that's the way I feel about it. I'm very, very proud to be here, working on this product and I really believe we can help businesses around the world.

Operator

We have no further questions at this time. So I will hand the call back over to Jack.

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

Well, thank you very much for coordinating; this was a very good set of questions. We appreciate those very much. We always like talking to our investors and I just like to make a couple of last comments. This company is the closest thing to a family I've seen out of any business I've ever worked at. I really enjoy working here and I want to put a shout out to all the employees of INTRUSION for their hard work, their dedication and their excitement and their zealousness about stopping cybercrime. I think they're doing a great job for America and I'm really, really proud to be here working with them.

We are doing some upcoming things that you may want to be aware of. There is an Annual Shareholders' Meeting, May 18th, there is a Needham TMT Conference on May 19th that I'll be participating in and the very exciting Black Hat Security Conference July 31st through August 5th is going to be live and in-person this year and we are a senior sponsor in that event, and we are very excited about the exposure we're going to get, the exposure the market is going to get to what Shield really has to offer and that set of highly technical audience. So I know you're going to want to participate in that if you can. Thank you so much. Have a wonderful evening. Goodbye.

©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

Operator

Ladies and gentlemen, this concludes today's call. Thank you for joining. You may now disconnect your lines.

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.

