INTRUSION Inc. (INTZ) CEO Jack Blount on Q2 2020 Results - Earnings Call Transcript

Aug. 14, 2020 9:19 PM ET**Intrusion Inc. (INTZ)**9 Comments2 Likes

INTRUSION Inc. (NASDAQ:INTZ) Q2 2020 Results Conference Call August 13, 2020 5:00 PM ET

Company Participants

Mike Paxton - VP, CFO

Jack Blount - President and CEO

Joe Head - Senior Vice President and Co-Founder

Conference Call Participants

Howard Brous - Wellington Shields

Operator

Ladies and gentlemen, thank you for standing-by and welcome to the INTRUSION Inc. Second Quarter 2020 Financial Results. At this time, all participants are in a listen-only mode. And after the speakers' presentation, there will be a question-and-answer session. [Operator Instructions]. And please be advised that today's conference is being recorded. [Operator Instructions].

Now Mr. Mike Paxton, you may begin.

Mike Paxton

Alright. Thank you. Welcome to this afternoon's conference call to review INTRUSION's second quarter 2020 financial results. Participating on the call today is Jack Blount, President and CEO; and Joe Head, Senior Vice President and Co-Founder. I will go over financial results and Joe will give a business update and review current projects. Jack will give a business update, including our current and future market conditions. We will be glad to answer any questions after our prepared remarks.

We distributed the earnings release at approximately 3:05 PM today. A replay of today's call will be available at approximately 6:30 PM tonight for a one week period. The replay conference call number is (855) 859-2056, conference ID 9435598. In addition, a live and archived audio webcast is available at our website, intrusion.com.

Please be reminded that during this call, including the question-and-answer session, we may make forward-looking statements which reflect management's expectations regarding future events and operating performance and speak only as of the date hereof. Forward-looking statements involve a number of risks and uncertainties. Such statements include without limitations, statements regarding expectations of future revenue, product orders from new and existing customers, and profitability, and are qualified by the inherent difficulties in forecasting future sales caused by current economic conditions and spending patterns of, and appropriations to, U.S. government departments.

Forward-looking statements also include the effects of sales and implementation cycles for our products on our quarterly results and difficulties in accurately estimating market growth, the unpredictability of government and corporate spending on information security products, production revise and the effects the coronavirus, as well as other statements.

These statements are made under the Safe Harbor provision of the Private Securities Litigation Reform Act of 1995 and involve risks and uncertainties which could cause actual results to differ materially from those in forward-looking statements. The factors that could cause actual results to differ materially are detailed in the company's most recent reports on Form 10-K and Form 10-Q, particularly under the heading Risk Factors.

Now let's move onto the financial results. We had a net loss of $715,000 in the second quarter 2020 compared to a net income of $1.8 million for the second quarter 2019 and a net loss of $465,000 for first quarter 2020. Revenue for the second quarter was $1.7 million compared to $4 million for the second quarter 2019, and $1.8 million for first quarter this year. Gross profit margin was 61% in the second quarter 2020 compared to 60% for the second quarter 2019 and it was 58% for the first quarter of this year.

INTRUSION's second quarter 2020 operating expenses were $1.7 million, compared $0.7 million for second quarter 2019 and $1.5 million for first quarter 2020.

Thank you. And now I'll turn the call over to Senior Vice President and Co-Founder, Joe Head. Joe?

Joe Head

In the previous quarter’s call on June 12, we were still in the shutdown. From a government customer standpoint, they're still not very open. Our government customers are in a mixed state still, many are still working from home. Some are working partial schedules and others are back to work. Common missing element is procurement departments are not back to normal. I've talked to the customer who had the $2.4 million contract with us last year. Nothing is moving forward on that as of yet.

But we have started up a new business during the play. We have won new contract for $375,000 ready for award, and a good rumor that a budget has been approved for another contract for about $800,000. Also, we teamed with another company on Air

Force contract called the Advanced Battle Management System, our partner company has awarded spots on the $950 million IDIQ last week. They'll give us a potential new customer for TraceCop, as well as some other AI projects. Again, this is a IDIQ, where it's no guarantee, it’s been than ever, but it gives us a contract vehicle. And we were on the winning team to do some stuff that the Air Force liked well enough to pick our team. We expect renewals from existing customers to auto renew, even with partial staffing. So those are all proceedings from where I can see all normally. So I don't have any renewal threats to report. So I think that's pretty good.

So at some time in the future, we expect the government to return to normal operations. And so our pipeline are reported sometime back of new DoD opportunities will move forward for new business as things turn back to normal. So we've got several good ones there. And as usual, we have plenty of bandwidth to keep our own customers happy. And we have new projects defined for new funding as they awaken and return to work. As I mentioned a couple times before, the goals of a defender is to make it harder for an adversary to penetrate to operate and to remain undetected on their network. So historically, our Savant and TraceCop and STA products only address two of those three items to operate and remain undetected. But it was a reporting service that find things after the fact then you have to go fix them.

And as some of you know, our team is conceived, developed, tested and done a ton of innovation for our new Shield product family since February. My patents write up was over a 130 pages two weeks ago, and we expect to the provisional filings to be ready to file with the patent office tomorrow. I did spend a lot of time on this family of products, which have their roots in both Savant and TraceCop, go far beyond anything in the world and scope, coverage and effectiveness. The great news is that now we're only days away from patent filing so that we hope patent coverage, and we’ll be able to start describing more details as we begin Beta testing with customers on September 1st.

I've been using Shield for all of my network traffic for more than a month now with over 6 billion rules working and live in real time, blocking bad stuff in real time and reporting it. I'm pretty excited about the product and how big this innovation will be in the marketplace. The purpose of Shield is to make it harder to penetrate the network in the first place, and harder to spread inside an enclave and very hard to operate and remain undetected by changing the approach radically and doing blocking in real time, using huge data, AI and this process gets smarter every day. So, unlike a lot of rule based systems, this thing learns and gets better as it operates.

For sure this is what all antivirus and security products are marketed to do, with the ongoing number of breaches and huge sums being paid to ransom where criminals underscore that the world's current enclave network, desktop and post penetration defenses just aren't working. This new set of Shield solutions are novel and greatly reduce the number of adversaries and methods that can stay in the compromised game. Shield is a family of products which are built on each other and offer ever increasing protections to cover additional environments and threats with each additional release. And best of all, they're not do overs but incremental steps that aren’t huge developments from release of the first Shield to each additional stage.

I'm very amazed what our team has accomplished during the COVID-19 interruption. We have folks that come in every day and a ton of folks that work from home 100% and their work output has been tremendous. If anybody believes that folks working remotely are less productive, that has been far from the case here. Our team rocks and has amazed us every day. Shield has many moving parts and innovations that are all working together well. Jack and I are very excited for the company's future as we launch the family of Shield products. Jack?

Jack Blount

Thank you, Joe. I think Joe has done a great job of trying to give you an overview. Just a couple of things I'd like to add and then I'd really like to be able to answer your questions. First of all, I'd like to tell you, I went out and spent a week in Washington D.C. about three weeks ago. And I went up there to meet with our sales reps. I went up there to meet with some of our customers who were willing to come in and meet with me. And to really find out what was going on in D.C. because I was tired of reading the newspapers and listening to the television. I was actually shocked to find out Washington D.C. is much more shut down than I ever imagined.

That to share with you just a brief view of that. I stayed in the Marriott Hotel Downtown that I've stayed in almost every time I go to D.C. for the last eight years. It has 1,500 rooms, and it's normally sold out unless you booked three weeks in advance. I booked three days in advance. I got there and found out there was only six rooms occupied in the entire hotel. Six rooms, Downtown Marriott normally sold out. I rarely saw a person on the street. I rarely pass the moving car on the street. I did have very successful meetings. I met, for example, with executives in USDA, that I used to work with and know personally. And we were in 1 million square foot, six storey facility in downtown Washington D.C., normally occupied by thousands of USD federal employees. And I found out there was four people in the building. There was a security guard that led us in through one door out of 12 doors to the building. And it was a two people I met with and myself. The building was empty. No other week, two months into this COVID crisis. I think that reflects for you what we're dealing with, with our customers.

Now, I did meet with a couple of our customers. Again, we don't talk about them personally, but they're all DoD side of the house customers. They were very gracious to meet with me. I spent an entire half a day with one of the customers with a roomful of very senior people in the agency. They love our company. They love the reports, we get them. They were devastated by the shutdown that they're dealing with. They ensured me that the build-up of demand for reports has not diminished and that they expect to give us in later third quarter and fourth quarter the quantity of reports they have planned in their original budget for all of 2020. So we will be extremely overworked the rest of the year if that business comes through as they assured me it would.

That was pretty generally the report I’ve got from every customer I met with. It was great to meet them in person. It was great to see their long-term admiration for this company and the work that we've done for them over the years, and their strong interest in our long-term relationship continuing. So I feel really good about that side of the business.

Even though Q1 and Q2 have been extremely painful, they've actually been a lot more painful for other businesses in this industry as you're aware. The number of business bankruptcies are way up. The number of business suicides are way up. We are living through a time that America has never envisioned before. I remain extremely optimistic. I remain extremely positive about everything we see.

One of the reasons I'm so positive is, while I hate to say it this way, cybercrime has also grown 28% according to the statistics in the last six months, grown. That's because of COVID. Almost every newspaper out there has ran an article on their front page about how cybercrime has gone up in the last six months. They are capitalizing on the fact that America is disorganized, is off balance and working remotely.

The fact that cybercrime continues to grow ensures me that the market for our products, demand, grows as well. Shield will be the first product I'm aware of introduced to the market that is a plug and play product. I've been selling IT technology literally for 40 years. I started out at IBM. I can tell you there are two major complaints about every IT product I've ever been associated with, including the ones I've bought, while I was the CIO in the federal government. Problem number one, they're way too expensive. Problem number two, they're way too complicated to install and operate. If you talk to any IT professional, they'll tell you, whatever IT products you're buying that cost you X, let's say it's $1 million, because a lot of the products I've bought as a CIO were $1 million. They say, you'll spend $4 million over the next two years, installing, configuring and maintaining that product.

So your $1 million purchase is actually a $5 million commitment. That's typical of IT products and why the market is so frustrated. Shield will not fall into that category. We have designed and implemented Shield to be low cost so that every business, large or small, can afford Shield without having to think twice about it. $2,000 up to 100 users and $20 a seat beyond a 100 users. Very, very affordable for a product that can literally save you bankruptcy, millions of dollars, et cetera.

So I think it's revolutionary in that regard. I also think it's revolutionary in the fact that it's plug and play. It's the only IT product I'm aware of that you can take out of the box, plug it into your network without reconfiguring your network, without talking to your CIO, without getting 17 other IT professionals to come in and work on it, you simply turn it on and it starts protecting you one minute later.

So I think we've overcome the two major obstacles of all IT products. It's now affordable and it's now installable. So I am increasingly intensely excited by how well the product works, by the magic it performs and about how safe it's going to make America. $3 trillion the world lost last year alone to cybercrime. That's 6 times more than all the bank robberies in the world added together in one year. And it's forecast to be $6 trillion two years from now. It's a growing massive problem. We're addressing this head on and we're addressing it with artificial intelligence. The only way that problem could be solved.

Fortunately, what I found here that is the reason I'm the CEO today is when I got here and looked at this company and met with Mike and Joe, I saw TraceCop for the first time in my life. And as an IT professional, who has worked in it for 40 years, who ran one of the largest data centers in the federal government for four years, I told them I'd never seen such a rich, robust database. And I immediately thought of the endless ways to monetize it. The first way we're monetizing it is with the Shield product. The Shield product could not be launched if it wasn't using the TraceCop database. That's 25 years of research that we're leveraging in one product.

The other thing I found two weeks later that blew my mind was Savant. Savant is the most sophisticated network appliance I've ever come across that real time analyzes every packet of data coming on and off of your network and stores into the database. Now, again, I saw that as an asset that the company spent 10 years developing, perfecting enriching, that could be coupled with TraceCop, that would -- could be used not as a log but as a real time defense mechanism. So what we have done is we've developed a layer of artificial intelligence that at the millisecond works real time, not later on logs, not weeks later finding decisions, but on the fly can make a decision about what it sees, about packets of information, determined that they're bad and block them.

Number one problem with all IT cybersecurity products today is all they produce is alerts. When I was in the government, we got from 50,000 to 500,000 alerts a day. Human beings cannot process 50 to 500,000 alerts a day. It's impossible. And so most of them -- almost all of them get completely ignored and every layer you add, you know there's another product in the market today that's growing very well because it advertises that it's all AI, big differences.

Number one, it costs you a whole lot of money. Number two, you have to sign a three year contract. Number three, it's only a logging product. It creates massively more alerts. I talked to a Gartner expert about it last night, who is very involved with this product, and I said, yes, but does it protect you from anything? And he says, well, if you act on all the alerts, you can make yourself safe. And I said, so how many new alerts does it produce a day? He says, well, I was at one company, and they got 10,000 a day. And I just looked at him in silence and said, who can manage 10,000 alerts a day? Shield on the flip side, would take those 10,000 alerts and block all 10,000 of them, leaving you nothing to do in IT and leaving your network safe. So we're not just another log or not another alert, or not going to create more confusion and chaos. We will block everything bad that's going on and make your network safe. And we do it in real time, at low cost.

So I believe the market for this product is, every business that uses the Internet, I believe it will grow rapidly because of the fact that you buy it, you try it, you like it, you're never going to take it out. So I am more excited about this product than any technology I've worked on. I believe this is a game changer technology in this market. And as Joe mentioned, we can't talk too much about futures. But please understand, Shield is not a one off product. Shield is beginning of a family of technology that will also use TraceCop, that will also use Savant, that will also have a layer of its own specific AI that

we will have another half dozen products in the family by 12 months from now. Because they're all fairly small, they're all fairly powerful, and they're all added.

One of the things that I get asked by every analyst that I try and explain Shield to, says, well, what about the cloud? Everybody is going to the cloud. This is an enterprise product. And I say, how many businesses in the world have a local area network that they have to secure today? And I get answers of anywhere from 30 million to 10 million depending on who you're asking. But it's a huge number of businesses. Lands haven't gone away. People still have them. They still have equipment, they still need it secured. That's why we're addressing that market first, because it's the largest, lowest hanging fruit in the most pain. The FBI again reports 60% of businesses in America hit by ransomware in 2019 went bankrupt, went bankrupt. They didn't just lose money, they went bankrupt.

So I feel a moral obligation as well as a business opportunity to attack this low end market first. But the cloud is growing. The cloud is very important. And our very next product in the family that we will be launching will be a cloud solution. It will be priced differently. It's still going to be affordable. It will be a service, it still will be plug and play. So this is a very, very important market that we're just breaking open. And we're going to continue to leverage Savant and TraceCop long into the future.

I know I covered a lot and certainly want to answer your questions. But I hope that gives you a better understanding of why Shield is so significant and how desperately needed it is by the market today.

Thank you for your time. Let me answer your questions.

Mike Paxton

Yes. Operator, can you remind the participants how to queue up for questions?

Question-and-Answer Session

Operator

Yes, sir. Thank you. [Operator Instructions]. And we have our first question from Howard Brous from Wellington Shields. Your line is open sir.

Howard Brous

Thank you. Jack, once again, congratulations on joining the firm and becoming CEO. I have a couple of -- and I'm excited about this business as you are. So, I would like to get back to the base business. And just if I can get a sense of what you're referring to in terms of either the third and fourth quarter of this year or some sense of assuming that the government is open, what we could be looking for in the base business in 2021? Your choice of either one.

Jack Blount

Yes. Well -- and if you look at the third and fourth quarters, I said, what I was told by our customers that I was able to talk to in person is they have a built up demand for reports that they're not able to push through procurement in the past five months, that they plan to be able to execute in third quarter and fourth quarter that will consume the amount of money they have budgeted for this company in 2020. So, we anticipate we have staffed and are ready to be extremely busy in our consulting services in third and fourth quarter meeting that pent up demand.

Again, cybersecurity has not stopped because of COVID. It's gotten worse. Therefore, the government's need for our resources is greater than it's ever been. They simply can't get anything out of procurement right now. I was assured by a senator and several other government officials that I met within D.C. that procurement is going to be open in third quarter and that they will be issuing things. So, I'm continuing to be very optimistic that third and fourth quarter will come in very positive and our numbers will be very close to what we forecast originally for 2020.

Now when you ask about 2021, I am even more bullish about 2021. Again, cybercrime we know is growing rapidly. Therefore, the demand for our traditional work out of the government will grow as well for 2021. One of our largest contracts that we've had for many years, I got a handshake agreement, will be signed in the next 30-days and will be renewed for another year. That's a multi-million dollar contract that we depended on. That was certainly in question that I was given complete confidence will be signed, and we will have that revenue. So, I'm very bullish that the government business is going to kick back in and be very aggressive, because demand is going to be even higher.

In parallel to that, we will have launched and have in the market a successful commercial product that could be sold from anyone, from a small company up to an enterprise. We anticipate having a Fortune 100 company as part of our Beta process right now. We are signing the final deals on getting that closed. So again, whether you're small, which is where most of our customers are fitting in, because we’re focused on the SMB market for Shield initially, because it's the quickest market to sell in turn.

If you talk to a Gartner expert or if you talk to a Forrester expert, they will tell you selling an enterprise IT solution into a Fortune 500 or Fortune 100 company is an 18-month to 24- month process. And you have to meet with and get approval from 18 different people. I've lived that world, I know that's true. We’ll win a lot of that business longer term, but that's not going to turn first quarter. So, that's why we're focused on SMB because SMB is decided by the CEO or the CFO, and those people are in pain. They're in need, and we have an affordable solution. And unlike the Gillette Razor is cybersecurity, try it you’ll like it. Put it in, run it for a month. Just to tell you how significant and this just popped in my mind, I brought Mike into Joe's office last night to give him an update on Shield desk. And I wanted to show him one of the new interfaces we developed by the way, that end users can look at to see what the product is doing for them, and we looked at it and we saw a lot of blocks happening. And again, it's very visual. It describes you what's going on, about 52 things, well, exactly, 52 things actually, popped up on the screen while we were standing there talking. And Mike says, that's pretty impressive. How long has this been running? I looked at the timer and I

said, Joe reset it 8 minutes ago. In 8 minutes, on our secured network, here in Richardson, Texas, we have 52 breaches that Shield blocked. That we were all three in the room, we saw it. It's amazing. That's amazing. That's how the product works. This product is going to sell like crazy. And I am very, very bullish that we will see phenomenal growth in new sales in the commercial market. Deos that answer your questions Howard?

Howard Brous

Fortune 100 company is public?

Jack Blount

Yes, it is.

Howard Brous

Okay. In the 10-Q, you referred to -- just a couple of items. Value-added resellers and system integrators, the market share for the target market. You're talking about Ingram and people like that?

Jack Blount

Yes, we are.

Howard Brous

Have you spoken with Ingram?

Jack Blount

I have spoken with Ingram, I have spoken with two VPs in Ingram. I've met with Tech Data, I've talked with one SVP at Tech Data. They are very excited to get their hands on the product. They say, it's going to be very easy for them to push this through their channel. Again, I got myself in the back a second, but you can look in the history books. I helped create the channel back in 1985 at Novell. Novell is really the first company that identified and grew and matured the channel. We grew from originally three resellers into 2,000 resellers and 19 distributors in six years. I've used that channel in every company I've gone to since I left Novell. I know it well, I know how effective it is. The reason it's so effective is there's 34,000 resellers around the world, all who have existing relationship with 90 million businesses around the world. So you're not cold calling ever. You have an experienced rep with an experienced relationship with the customer walking in and saying, I have virtually no cost product that will solve your cybersecurity problems. Let me show it to you.

So I think the channel will be extremely effective at moving this product forth. Now in addition to that, and to prime upon, we have telesales people who are making calls today, signing up customers and Shield is not even shipping yet. I talked to five

customers that came out of that telesales this week in person. And these are five real customers that are waiting to get the Shield product. Typical businesses all across America, one of them is Gartner, one of them is a manufacturer, I mean they're very diverse. Again, I think we fit every company's need. So early signs are that the customer understands the problem, and then the customer understands our solution.

Howard Brous

So my last question Jack is, basically Beta testing starts on or about the first week September, when you're finished, second, third week in September. Can we expect to hear from you publicly, as to the results?

Jack Blount

Absolutely. You will hear from me. Officially the Beta in the contract that they're signing is a 30 day Beta. So it will run through the end of September, but I will get feedback before the end of that. So I plan to publicly talk about the Beta program, probably midway in the third week of Beta once we have enough data to give you something meaningful. And then again, in the fifth week after we close out the data and have all the formal results.

Operator

We have our next question. Please state your first and last name and the company name. Your line is open.

Unidentified Analyst

Aaron Warwick, [Diaz Capital]. A question for you about the Alpha testing, how many companies were involved with that?

Jack Blount

We really don't talk about Alpha testing. We have a non-disclosure with those customers, so we really can't disclose that. And again, Alpha testing, several people have asked me about it. I've been doing this for 40 years. I don't know if anybody who's ever really exposed Alpha testing. There’s a lot of bugs found. There's a lot of things fixed, there's periods that it goes down because you have to fix bugs. And that's why we don't track and report on Alpha testing because it's too hard and too difficult for non-software developers to really understand. I feel like it's been a very successful Alpha test process. Again, I can't tell you how many bugs we closed, that I know it well over a 100 and I can tell you that's not alarming. Most products I've worked on closed 200 bugs during the Alpha process. So a large number of bugs is very normal in Alpha.

Again, this is an extremely complex product. We are working at the millisecond speed, making analysis and decisions on whether to pass or block a packet of information. The AI that goes into making that happen, the decisions that have to be factored in is

extremely complex and there's therefore a lot of ways that can go wrong. So you have to do extensive testing to find all of those. So that's what Alpha is about.

Joe Head

If anything else going through is the competitive analysis team here, and we found one of the competitors that wrote their evaluation of their competitors, they said we have more than 30,000 signatures in hours, and had less than 30,000. Well, as of today we had 6.3 billion and the one that's running in the closet over here that I'm using, when you start looking at list of that size, it's interesting. Just pruning of the list and formatted properly and it load all the way. And it's been -- we're dealing with immense lists that are running at real time. And it's been a pretty amazing that it's been as smooth as it has.

Unidentified Analyst

I appreciate that clarity. And I think, that's what interests me, you said -- you mentioned the 200 bucks versus 100. I mean, stuff that I've heard from speaking to people in the industry, it sounds like -- and just from looking to the timeline from when you guys introduced Shield to the public to now it's been pretty quick. So I mean, it must have been a pretty, pretty successful Alpha test to get the Beta rolling this fast.

Jack Blount

Absolutely. It has been extremely successful. And again, that's because it's built on a database that's been around for 25 years. That's very, very mature that we can depend on. It's built on a Savant network appliance product that has been around for 10 years, has been updated eight or nine times, Joe?

Joe Head

Numerous.

Jack Blount

Numerous times. So it's a very mature product. If those two things didn't exist and weren't that mature, then we would not have been able to move this fast, the Beta would not have gone this fast. Another way to look at results for example, is I told you Mike and the eight minutes and I think that's a pretty telling story. One of our Beta customers is a Fortune 2000 business and in the one month period that they were in an Alpha test, we managed to block 1.2 million attacks for them. This is on a network that they thought was completely clean. They told us they didn't need our appliance and we weren't going to find anything. 1.2 million, think. No customer that has installed and looked at the Shield product has not found that it was blocking things within minutes. The attacks are real time, they're non-stop, and they're getting worse. Cybersecurity gets worse every day.

Unidentified Analyst

So when you look at the Beta testing now coming up, you've mentioned a Fortune 2000 company, you mentioned the Fortune 100 company. What are you talking about in terms of the number of seats that will be -- fit that Beta testing?

Jack Blount

Yes, I'd like to know, then tell you that. That is the reason we don't have a signed deal yet. They're trying to decide how much of their network they're going to expose. Again, the bigger the companies are, the more resistant they are, the more afraid of new things they are. So just because they're a Fortune 100 company, they're not going to open up their whole company to us day 1. So they're going to come back and tell us what part of their company that they're going to expose it to. I'm anticipating that most of these customers will be in the 200 to 500 workstation range during their initial Beta phase. But I think they have the potential to go skyrocket from there once they see it work and get convinced.

Unidentified Analyst

Yes. I appreciate that insight. That's good to know that 200 to 500 per company. So when you -- I'm assuming based on how successful Alpha was and how successful Savant and TraceCop have been. The Beta testing is going to go very well. So my question about that is building up the sales channel, how do you plan to fund that, is that something that you guys can fund on your own now. And you have to look to raise -- do an equity raise, take on some debt? What are you thinking with respect to that?

Jack Blount

Well, again, we have very solid plans right now, as we said before to fund the sales of Shield organically. We have money in the bank. We have a plan of how we're going to get there. It does cost money, we are spending money but we're doing it cost effectively. I'm not going out hiring 100 salespeople tomorrow and seeing if they can be successful. For example, I've hired a firm that does tailor sales, that has an amazing track record, that does work for Dell and Cisco, that's two of their customers that they allow me to name, very, very successfully. So they're very successful company. They know what they're doing, and they're already producing consumers for us.

So, their feedback to us after their first week was pure joy. They said it was the easiest product they had ever started selling. Again that's one week but we did turn on and stick it. We can turn it up as fast as we want to. We obviously pay based on the number of telesales, people we have. You want to start out small with a half dozen people. So, you can really manage the data, get the feedback, analyze what's working, what's not working. So, that's the process we can grow. It's a very affordable process. Again, you're not staffing people, you're not doing facilities. Telesales is a huge market that everybody uses today. It's become a very, very cost effective channel. So, we will grow that quickly. And we will grow it based on results. So, it'll be paying for itself as it grows. So, whatever additional costs we add basically are paid for by the new sales.

Unidentified Analyst

Good. And what are your thoughts -- I mean, obviously, this is geared right now towards the commercial space. But I mean, is this applicable also in the government space where you're currently operating, where I know you have a lot of contacts, other people in your business have contacts? Is that something that they're going to be interested into?

Jack Blount

Absolutely. One of the meetings I had when I -- one of the main reasons I went to Washington D.C., is, again, I have, unfortunately a customer that I can't name, they are in the DoD side of the government. They've spent two hours just talking about Shield, and they expanded from the start of the meeting, over 1,000 seat installation that they want to discuss with me to talking about a nationwide rollout that could potentially include they said 20,000 seats. Now, that's an opportunity. It's not a contract, right? That's what the customer

told me in a meeting. So, again, I think it speaks to the fact that yes, the federal government is going to be very excited. No other product -- I'll say this, I'll challenge anybody to prove me wrong. No other product stops the problem from happening. All other cybersecurity products that are used this way create endless alerts, that you then have to staff and manage and deal with. And you get the alerts so fast, you can't manage them and everybody knows that. We're the only people that say, what good are alerts. If it demeans on a work, it should demand to be blocked. Thank you.

Unidentified Analyst

Yes, that's and I -- like obviously I'm not a company insider. So, I can't say how the product actually works. Taking your word for it right now, but I can tell you that of all the cybersecurity people I've spoken with, they have said what you said and that is that this is a product that’s needed. And it's something that is currently not being done. So, anyway, I appreciate you guys’ transparency. I know sometimes you're not able to say things. I respect that 100%. But I do appreciate all the commentary you've given and how you try to be transparent with us. So, thank you very much.

Joe Head

One thing I'll add just for fun is we haven't said on this color lately, but firewalls and all the other products stop stuff from coming in. And one of the things that we've been amazed with is we're watching what leaves, stuff initiated within the enterprise. It's just throwing out to the Internet as a result of whatever. And if there's not another product that actually is doing that, looking at what's going out, and that's the thing that matters.

Jack Blount

Yes, again, the myth is that all attacks come from the outside in, the reality of working in the federal government for four years of working on cybersecurity my whole life, 80% to 90%

80% to 90% of all intrusions are caused from something inside going out. The outbound traffic is where almost all harm happens. It starts with simple call homes to pop up. But we stop all of those.

Joe Head

And more than half detect now are actually not malware. They're malware free, which means they're already on your system. It was on there when you bought the system, or they have a password backdoor, our product does both. But primarily, we're addressing the -- it calling out, we kill it, and we kill it in real time. So it's going to be amazing. It's not us against the firewall or us against the IDS. They do that, we do this. We found something they didn't. Would you like to renew?

Operator

We have our next question from Ross Taylor.

Unidentified Analyst

A number of questions both covering the core business and also Shield. On the core business earlier this year I think the call you had back late February, you talked about the ability to add $12 million to $16 million in revenues through the efforts of your new salesman and the like inside the government -- the federal government. When you're talking about the numbers, you think you can see, are those the numbers you're talking about being able to exit this year with the run rate at?

Joe Head

Yes. If I recall those numbers and update them for you, we had about $6 million to $8 million that were tied to the new sales guy that we hired, and all those customers. One of those is the 100,000 I just mentioned, he was actually a secondary one. There's one for about $2.4 million. And his whole team is in the flying around and checking for breaches business and they're not flying anymore. So, most of that I think is on pause, awaiting return to normalcy. But none of those have said, I don't like you or your mama or your cousin. They're all in the category of we’re close.

And -- but one of those actually -- actually two of those, one, we already got the order and our billing, the 800,000 will be the next one. So my comment would be that I would take -- the numbers are reported before and said that those are still there awaiting a pulse from the patient, which is the government got back to work. But we've had -- these others are reported are -- [DRK] is one of them.

Jack Blount

But again, not to mislead you, as we said in the press release, where we're seeing the biggest slowdown in delays is in new business in the government. The renewals are good. The new business is dead. The new sales guy I met with him when I was in D.C., I visited with three of his customers personally. They like him. They're anxious to work

with us. But they're virtually shut down. Again, these were companies, agencies, whatever you want to call them, that there was nobody there basically, me and the sales guy and the customer. The government in D.C. is shut down. It is depressing, but it is killing new business. But it's not killing the demand for the new business. So I think that demand will fire up, when it opens up, and it will be faster than it would have been before. So we're going to continue to pursue it.

Unidentified Analyst

Yes. Do you see the end of the federal year driving new business? I mean, historically, the government -- if you're running an agency, you don't want to leave money unspent. Is that going to be something you think that drives it? So we would see something in -- pick up in late September or is it something that, because they're literally just not there, this is going to be a unique year and people might not be able to spend their budgets?

Joe Head

It won't be really [dead] to me.

Jack Blount

Yes, no, it's a, it's a unique year. There's no doubt about it. I said at the start of this call, the world has never seen anything like COVID and the impact on the world. This is a one of a kind, a disaster in any aspect, 52 million Americans unemployed. Come on, we have to realize how bad things truly are. So my other experience from being in the government is that they will not be able to spend their budgets in the third or fourth quarter, the way they have in past years. For one thing, Trump is not our past President. Trump has reallocated money continues to reallocate money, like no other President. And when it's saying they're unused quarter after quarter, I can guarantee you a lot of us getting reallocated. It's the way demand works. It's the right thing to do. It doesn't make sense to try and race through spending two quarters worth of money in one quarter and not expect people to misuse it. So, I think he's being what we'd want him to be as a good President, don't get me wrong, but I do think it will have an impact on new business.

Unidentified Analyst

Okay. Now you guys developed the product along with an individual or a team inside the DoD and that product seemed exceptionally sophisticated and unique. How does that product parallel? What you're doing with Shield? How does it differ?

Jack Blount

Sure. The one that I jointly thought up with one of my DoD buddies was basically a software implementation of a Shield like thing that runs on every workstation, in a virtual machine. And what Shield does is basically collapses that to an appliance, it's in every way I can think of easier to support, easier to deploy. My deal with them still is if they want to deploy that one throughout the DOD, they certainly can in the base, the base --

their part without our enrichment, they can do for free. But then they can buy subscriptions to us. I've stayed in contact with my buddy there. I don't know how the Shield will launch and do well. That one will probably come to deployment as well, but they won't be able to do their work until they get back to work to start.

Unidentified Analyst

If it were rolled out to other branches of the government, would you then be compensated for it being rolled out? It's only the DOD that gets to roll it out for free?

Jack Blount

So their basic function doesn't do a whole lot but some -- all of the enrichment that uses TraceCop, they would subscribe into including DoD.

Unidentified Analyst

Now, so basically it becomes a force multiplier for new business for you as well.

Jack Blount

That is correct.

Unidentified Analyst

And it also becomes a data gatherer additionally, correct?

Jack Blount

And you know, it could be a mandated federal thing if it's a mandatory rollout for free, with an optional upsell, which is positive, but I don't know what the timeline for them doing their half is since they're shut down. But I suspect that it'll come back to be helpful.

Unidentified Analyst

Okay. And with regard to Shield, how much capital do you see needing to deploy to bring that through the Beta test to where you can bring it into the marketplace?

Jack Blount

Very little. I mean, the development is done, the money spent is spent, the development is done, the product is ready to ship. Well -- but we have a partnership with Dell, a company I've worked with since 1985 when I met Michael Dell in his dorm room in Austin, Texas. And I've used at multiple companies, to where Dell will provide us products to customers. And no direct cost to us initially. And therefore the cost is amortized through the service fee. So we don't have to spend a lot of capital to put hardware in customers' location. Dell will bill those customers' products without us spending any money. So it's a great partnership, it's a great product. There is no better

hardware than Dell. All my partnerships with Dell have been successful. That's why I went to them. The customer is assured of getting a solid reliable product with a warranty and a service agreement and a service company behind it. So, I think it's the absolute best possible solution we could have if we were in the inventory business, building and stacking and shipping hardware. Our CFO just turned white as a sheep.

Joe Head

Done that before.

Jack Blount

We've done that before here. We don't want to go back to that world. So again, we're not having the capital expense on that front. We have strategically outmaneuvered that.

Unidentified Analyst

Okay. So when you look at your product, and you look at a Fortune 500 company, that takes something that has 40,000-50,000 employees or more, how many seats do you think they potentially have that would make use of this product? And is this the kind of thing that you see the company with like -- or federal agency that has 100,000 employees who log into computers? Do you see this the type of thing that everyone who basically gets into the network is going to need because if they don't have it, they become a weakness?

Jack Blount

Yes. Again, at the price point that we have it is not a barrier to anybody implemented. The fact that it's plug and play, it's not a barrier to anybody implemented. I don't believe any of those organizations will start out with 100,000 people on it. But I think they'll all end up with 100,000 people on it. I don't know how a CFO or a CEO or a CIO can sit back after they've had this product for a few months and watch what it does, allow any of their workstations anywhere in their network to operate without it. I think it will become a requirement, a new layer that you add to what you're already doing that makes you safe.

Unidentified Analyst

So literally, you're looking at this market. When you talk about your addressable market, your realistically addressable market, you're talking -- you're thinking, not hundreds of thousands of seats or 100,000 seats. I mean by my math 100,000 seats at a 75% margin retaining, that makes you about $0.50 a share. But you're really thinking about millions of seats, aren't you?

Jack Blount

Absolutely. Absolutely.

Unidentified Analyst

And at millions of seats, will this be a 75% growth, a 37% net margin product for you? Will you do better than that, would you -- it sounds like you have the potential to do better given the nature of what you're doing?

Jack Blount

Yes, I think it scales. I think we'll …

Unidentified Analyst

70% gross.

Jack Blount

I think we'll do even better than that.

Unidentified Analyst

I used to be the CFO, I wanted to make sure you guide low.

Jack Blount

No. Again, as I said, I've never been more excited about a product from this. This is a largest addressable market I've ever worked at. When I went to Novell back in the early 80s, I think they had 50,000 users of NetWare on their network. When I left six years later, they had 12 million users on NetWare and the network was still growing. So yes, I think this is millions of users. And I think this is a lot more valuable than NetWare.

Joe Head

We only talked about the first two Shield rollouts, Shield for the home workers if it comes at number times 1.5.

Jack Blount

Yes, again if you want to talk about markets, you have talked about the family of products. One of the new markets that is developed out of COVID, that McKinsey is reporting as the new norm. That Gartner just sent out a report yesterday is the new norm. It's the mobile home worker, the teleworker is the new norm, they're here to stay, there will be millions of them. And every one of them need a new Shield product that will support them in their home environment. Shield 1.0 does not support the home worker. But that is part of our family of products, what we will be announcing is a product for every user in their home, both business wise and personally. So, technically, every user with a computer in America is a customer and really every computer in the world is a potential customer.

Unidentified Analyst

So, we don't need to ban TikTok we just need to buy Shield.

Jack Blount

If that goes out over cellular that would be a little bit hard.

Joe Head

Let me answer that a different way. Shield isn't going to ban TikTok -- block TikTok, if the business allows it. So, TikTok is not an issue, that is the virus, visually it's a virus that people trust. That's the problem. So, yes, TikTok should be banned regardless of whether you have Shield or not. You could ban it was Shield, but that would be a company decision. And right now companies are the ones that are using TikTok.

Jack Blount

So, definitely there's a difference between a company that's naive something that has a vulnerability, and a company that purposely designs part of a single private data into their infrastructure.

Unidentified Analyst

Now, you've got this market opportunity. I'm going to leave you with this question. How rapidly should we? I mean, it sounds literally like you're bringing something to market that almost sells itself like selling lifeboats to people on the Titanic. I mean, it's -- it seems like it's a home run, and it's going to be a real straightforward process that can lead to wild expectations. Are you going to fulfill those you see those wild expectations being reasonable to be fulfilled? How long does it take you 1 million people using this product?

Jack Blount

Again, I don't know none of us have a crystal ball. If you're asking me for Jack Blount's opinion, without any facts behind it, because there's no way to give you facts on this, 1 million people in 2021, I think is easy to assume.

Unidentified Analyst

I have to say this is I think one of the most exciting products that pretty much any of us have run across, and it really has a chance to reshape the cyber industry. Because when you do talk to the big players, and we have investments in some of the big players, this is not a thing that they really have even thought about being possible.

Jack Blount

I agree. Again, I am more passionate, more excited about this product than anything I've worked on in 40-years. I have recognized that because I spent four years in the government and saw the intense, extreme nature of cybercrime, cyber warfare and

where it was going. I started working on finding the solution. And when I stumbled into TraceCop and Savant, I stopped looking. And I simply added the AI to it. So this was meant to be. I think, it's needed by America desperately. And that's part of the reason we want to make it affordable. I mean, it's -- you don't have to sell for a lot of money to make a lot of money. You can make a lot of money, making less on a product that gives you a larger market. I'm much more about winning a large market than making a few customers happy.

Unidentified Analyst

When you have 1 million shares outstanding, you got leverage, right?

Jack Blount

Right.

Joe Head

We've seen this in America a couple of times where there's nothing about the product that doesn't last to make the rest of the world's life.

Jack Blount

So yes, I talk about America, who we're going after first. We file for international patents. So we've used Wilson Sonsini Goodrich & Rosati, one of the best law firms in the country for doing trademarks. They are filing our trademark patents for us. They are filing internationally. And again, if you look back at my history, I started out selling products at Novell in the U.S. When I started there a 100% of their sales were in the U.S. Four years lady later, 50% of their sales came from international countries. I have 8 million frequent flyer miles. I've been around the world. I have connections all over the world. I believe this is a worldwide product.

Operator

And we have no further questions at this time. Presenters?

Mike Paxton

Okay, then we'll wrap up the call. Operator, we appreciate it. There are no more calls, no more questions?

Operator

No further questions at this time, sir.

Mike Paxton

Okay. We'll wrap up the call. Thank you for participating in today's call. If you didn't receive a copy of the press release or if you have further questions you can reach me at 972-301-3658 e-mail mpaxton@intrusion.com. What's your e-mail jack?

Jack Blount

JBlount.

Mike Paxton

jblount@intrusion.com .

Jack Blount

B-L-O-U-N-T.

Mike Paxton

All right. Thanks, guys. I appreciate it.

Operator

Have a good day you all.