Stanford eCorner

Crowdsourcing Cybersecurity [Entire Talk]

Jay Kaplan, *Synack*

December 07, 2016

Video URL: http://ecorner.stanford.edu/videos/4859/Crowdsourcing-Cybersecurity-Entire-Talk

Entrepreneur Jay Kaplan, co-founder and CEO of Synack, describes how the idea of creating a cybersecurity service for enterprise businesses by crowdsourcing hackers went from sounding like a long shot to launching as a venture capital-backed startup. Kaplan, previously a senior analyst at the National Security Administration, talks about the virtues of government work and the nuances of “white hat” hacking.

Transcript

(audience applause) - Tina, thank you so much, it's great to be here. This is the last lecture I understand of the semester and usually save the best for last, so I thank you for that honor. (audience laughs) So I'm going to start off, today you're going to learn a lot, you're going to all be expert computer hackers by the end of this presentation. You are going to learn a little bit about cybersecurity and you're obviously going to learn about our story and what Synack does and how our company evolved over the years. But before we get started I want to tell you a little bit of a story of my own. Back in February 3rd, 2013, I was woken up in the middle of the night, it was about 2am, and my boss gives me a call on the phone and she says Jay, you've got to get to the NSA now operation unicorn is a go. What's operation unicorn? Well she can't tell me over the phone because everything's classified right? But I put on my clothes, I jump in my car, I go up 295 North about 25 minutes north of Washington D.C. and go into the front gates of the NSA, run into the Research and Engineering building, which was the building I worked in at the time. I sit down at a computer station, start looking at the notes I say yeah you're right operation unicorn is a go. I pull up a chair, we have other operators working on the project and I actually can't tell you anything else sorry I might have to kill you.

(audience laughs) But what I can tell you is that and I'm sure you're seeing this every single day, cybersecurity is a really big problem today. Company after company is getting compromised getting breached. You hear about the Target breach, you hear about the Anthem breach, you hear about Sony, JPMorgan Chase, you're hearing lately about these hospitals who are getting hacked and then hackers are basically locking down their systems and saying unless you pay us this ransom, we're not going to unlock any of the systems. It's a big problem and I think you guys are very aware of it now because it has gained such mainstream media adoption that it's something that we might've not thought about before but everyone's thinking about it today. And the threats are really everywhere, the real problem here is that the actual cybersecurity talent is not. We have a huge shortage in this industry. Right now there's over a million cybersecurity jobs that remain unfilled and over 70% of the security professionals within the organizations trying to hire for these positions are saying that this shortage does direct immeasurable damage to the organization itself. Frankly guys it's way too easy today to break into any organization's network, application, whatever you're trying to break into if you have the right resources, expertise, and motivation. Definitely learned that my time at the NSA. I was focused on the counter-terrorism mission basically tasked with targeting foreign terrorist communications and so forth.

It was an incredible job but it definitely opens your eyes and gives you a pretty unique perspective on the space. Today it's like bringing a knife to a gun fight right? The attackers are well-resourced, they have a lot of motivation, they have a lot of money, different states are ultimately funding this. So how does an organization that might even be smaller defend against these attacks? It's just not fair, right? Clearly there's a need and it's a need that we saw. So you're probably thinking to yourself okay yeah this is a problem for big companies right, big enterprises, JPMorgan, Anthem, all of these companies are huge. So who would want to attack a smaller company or who would want to attack maybe one of you guys. We did a little bit of an

experiment we said why don't we put just a random box on the Internet, not attributed to anyone or anything. This is called the Honeypot in the cybersecurity space and we said let's watch what happens to this box. Let's put down some tools, let monitor the traffic, let's see what people are potentially doing from the outside world. We opened up Port 22 which is basically the port used to connect to that remote machine from the outside and within five minutes we started to see unauthorized login attempts, we actually registered almost 100,000 login attempts on that machine. What does that say? It means that there is automated attackers all over the world just looking for anything that's vulnerable on the open Internet.

You can kind of see here it's a little bit hard to see but they're running through a dictionary attack, so basically going through the entire dictionary and trying to login using just random usernames and passwords. So I think this is pretty interesting, right? But I'm going to back up a second, I'm going to tell you a little about my story and how we got into this. So I went to school in Washington D.C. I went to GW it's one of the NSA's Centers of Academic Excellence at the time, there were only a few. They funded me through school and then ultimately I want to go work for them, so it's kind of life ROTC for cybersecurity geeks like myself. I left in 2009 after getting my masters and joined as a Global Network Exploitation and Vulnerability Analyst. Kind of described what that was before, I didn't really know too much at the time what that job entailed or what it meant but I went through quite a bit of training obviously was exposed to unbelievable projects, unbelievable missions, and I can say without a doubt I saved a lot of lives. The question at the end about February, March 2013 when I realized that there is such a huge problem in this world as it relates to cybersecurity and I had a revelation that I think I could solve this problem, I think I could solve it and I think I could pull out one of my really good friends at the agency at the time. And maybe we can start a company that addresses the big issue and I'll tell you more about how we're going to do that but I was also thinking maybe I should go to business school, maybe I don't have the right experience or maybe I need to learn more about how to run a company, never really ran a company of this caliber before. Or maybe I should just stay in the government you know it's such a cool job as being exposed to so many interesting things I was saving lives, I honestly think it's probably the coolest job you can possibly have in the federal government as a computer nerd.

I ended up starting Synack, I left, I joined an accelerator program out in Boston called Techstars, very analogous to Y Combinator. Went through that for a few months and then ultimately moved out to the Bay area in the middle of 2013 after raising a seed round out here. So for us, how do we solve this problem? We look to a trend that many of you are very familiar with today, I'm sure every single one of you in this room has interfaced with one of these companies probably within the past week. And it makes a lot of sense, there are a lot of resources out there in the world that we can leverage to solve problems. But thinking about solving cybersecurity using crowdsourcing that sounds crazy, right? Well it sounded crazy to us too, but we started to ask people if we created a solution like this would you actually use it? We asked real potential customers, we asked people back at the NSA, does this sound even feasible. And they said you know it does, but what you have to really think about are all the implications as it relates to crowdsourcing in the consumer space and you have to address those implications for business. And so there were five things that we sought to address. One, trust, these are hackers we're talking about. How do you trust a hacker? So we inserted a vetting process and Uber has struggles with this problem a lot, they say we do background checks on people and then, I don't know it's not very good. But we inserted a vetting process such that we do background checks, we do ID verification, we have to do this globally, we're in 40 different countries today and so we had to enlist the help of a lot of third party companies to help us do that.

We also vet our researchers from a skills perspective, we only want to work with top people and so we can't just say any Joe Schmo off the street come work for us, but we put them through a practical exam and a written exam to make sure they meet our minimum bar of skills. Scale, how do we scale this business? Ultimately there is like I mentioned, a shortage of talent in this space. And so for us, we recognize that in order to be a scalable company long-term we had to turn to technology, we couldn't just rely on people alone and so we decided to create an automation platform in conjunction with the researchers that we would be utilizing in order to automate some of the low hanging fruit attacks that they're throwing at our customers. And that has turned out to be an amazing resource for us and we've been putting a lot of engineering effort into that technology. Management, how do you manage hundreds if not thousands of hackers around the world and how do you enable customers to interface with them on an ongoing basis? Well we created a platform, we created a whole online interface where researchers can submit vulnerability data that they find on customers, we created an interface for customers where they can see what's happening and all the high-impact vulnerabilities coming from our researchers. And all of that is contained in one easy to use online interface, we even have a function for our own internal team to leverage interacting with both sides. Engagement, how do you keep, we call them researchers, by the way, it's kind of a little less scary than hacker, but how do you keep researchers engaged? How do you keep them motivated to find these really hard issues, what if they're only looking for the really easy stuff to find? So what we inserted was actually a bounty driven approach for conducting vulnerability research. So we basically said if you're a hacker and you go through a vetting process, you find a problem on one of our customers, we're only going to pay you if you exploit that customer, you find a vulnerability on that customer. And we're going to pay you based on the impact to that organization. So it really aligns the economics in a fundamentally better way so we're not paying them time materials, they don't get paid unless they're finding things and they're getting paid when they find really serious stuff a lot of money, we paid up to $25,000 for a single vulnerability so far.

And then intelligence, how do we make sure we understand what the researchers are doing? It's one thing to say okay we're getting lots of vulnerability intelligence coming from the researchers, but how do we actually know what they're doing on a day to day basis? And long-term, if a customer is getting more secure hopefully we're not finding anything anymore. So how do we actually prove to that customer that we're still doing work right? And so we have a whole analytics and intelligence platform that feeds real time data to our customers. So that's how we've addressed all the problems with crowdsourcing as it relates to the cybersecurity space, as it relates to hackers, so really really interesting. Not easy to figure all this stuff out by the way. And then comes the early days, we thought this all through we had a solution for everything, but we then realized shoot there's a little bit of a chicken and egg problem here, how do you actually find customers when you don't have any hackers and how do you recruit hackers if you have no customers, or no work for them to work on. It's a typical marketplace problem, and the way we solved it is actually by hiring some hackers, we basically paid them on an hourly basis upfront. We said we'll still pay you on this bounty-driven model if you find vulnerabilities, but at the end of the day we were able to bring them on board and convince customers we had a stable enough of a community to be effective when we started testing their environments. That doesn't look anything like me anymore I don't know. (laughs) But getting over the you're crazy moment. When we first walked into some of our early customer prospects, they basically said you guys are nuts, I mean come on who are you, what is this company, you're two random dudes from Washington D.C.

and you're asking me to basically employ hackers and they're going to go hack my stuff and they're going to tell me what the problems are, how do I trust them, how do I trust you, who are you? Well it turns out actually coming from the NSA it gives you a lot of credibility. And they start to listen and what we found was really talking about our experience at the NSA and telling them that this actually aligns to a lot of NSA's methodologies. NSA employs massive amounts of data, they use that data to largely drive a lot of their intelligence missions, they have really really smart and motivated individuals, those individuals are not paid that well, but the mission is so exciting that they're willing to come in even at two in the morning and work on these projects and so that analogy resonated with our early customers. And they said alright, maybe we'll give this a shot. Certainly we're not the first ones to say, trust us we're from the NSA, they're a lot of companies doing that. This was a Forbes article where they did a whole spread on Ex-NSA and ex Israelian intelligence folks that started companies, it was kind of cool they made me put on a trenchcoat. By the way I stood in front of a blue screen and then they photoshopped that together so it's not as cool as it looks. Anyway, so we started to mature, we started to go from that's crazy to wow, this might actually work, right? And the way we convinced customers to try it was say, we'll do a proof of concept or a proof of value with you. Just come in, we'll work for a seven day period, we'll launch our cadre of security experts at you we'll tell you some of the problems over that seven day period and we'll show you there's massive gaps in what you're doing today and what we're able to do for you. The problem we didn't anticipate, and this happened with on of our very early customers, was that some of their environments are so bad that it actually scared them.

So there was a pretty large company, we basically found over 100 vulnerabilities within seven hours, and that customer was like holy crap this is my job, is to protect this application and clearly I'm doing a pretty crappy job. And so for them, they actually went silent, we emailed them, we called them, they wouldn't answer our phone calls, and we're like what's going on, we thought we did a great thing here. But the reality is they were so scared that they refused to talk to us because they were scared of losing their job. At the end of the day we figured out other people in the company to go to and everything was okay. We mediated the problems and we ended up taking more of a low and slow approach, we kind of scoped out the work so that we'd do it a small piece at a time. And they're still a great customer of ours today, so it's a great success story, but it was a little bit scary right and we freaked out, we're like oh my gah did we do something wrong, are they going to sue us? Lot of crazy things happen in the early days of a company. Then came the F word of entrepreneurship, right? Fundraising, who doesn't love fundraising? So fundraising for us actually turned out to be a pretty easy process and I think a lot of entrepreneurs can't say that, but cybersecurity is just a space that is really hot right now there's a huge need for new innovative solutions. We are fortunate to align ourselves with phenomenal investors, we raised seven and half million dollar round in April of 2014 and then later on in 2014 we raised our 25 million dollar Series B. Google is an investor, Kleiner Perkins is an investor, and then we have some other great investors as well. So it's been a lot of fun to work with these folks, we definitely recognize that having a good investor syndicate is absolutely necessary to build a sustainable business.

They help you a lot, whether it's through customer introductions, whether it's through making introductions to executives to join the company, other talent, and to just give you a really good perspective on things because they've seen it before. And so we put a lot of value on aligning ourselves with top-notch investors early on. We also recognize that early employees are super crucial. You have to hire the right talent early on. And they have to really believe in the company's mission, it's one thing to say okay you're a hot Silicon Valley company, you have great investors, you're well-funded, it's another for them to really believe in cybersecurity, for them to believe in our approach, and to get behind the company in a big way. And so that was a big goal of ours early on, we wanted cultural fits, we wanted people who we wanted to sit down and have a beer with, not everyone, but you know how engineers are sometimes. (laughs) Hey I was an engineer I can make fun of them. And then what we also realized was that early customers are just as important, these are the people that are not only going to serve as references, as you continue to build the company but they're actually providing you a lot of really valuable feedback. And so you actually have to choose your early customers wisely, just because there's a huge bank willing to pay you a boatload of money doesn't

necessarily mean they're the right customer for you in the early days. You have to really think about who are the people within that organization and are they willing to give you both the positive as well as the negative feedback.

And those early customers really drove our product roadmap, they drove our vision, they helped us prioritize a lot of the future sets and we found that to be super crucial. Now we all hear disruption today right? It's like the big buzzword and it's kind of annoying you hear it all the time. But the reality is, unless you're actually doing disruptive unless you're actually doing something really different, people just don't care to listen. And certainly crowdsourcing security that was disruptive, it was very different people had not heard of that before. We placed on CNBC's Top 50 Most Disruptive Companies list, now for the second year in a row, we're now the number 20 most disruptive company says CNBC. I wish everyone put us on some list in the top 50 but it was exciting to be on that list none the less. And I think it really highlights the fact that doing something disruptive gets people to pay attention. And that's how we got our customers to pay attention. So who's actually trusting Synack today? Well we're very focused on large enterprises, so we're working across the Fortune 500, we're now working with a lot of international customers in a variety of different countries. We're touching government, we have a lot of financial services customers, it's one of our heaviest industry bases.

Technology, consumer goods, retail, I know you've seen a lot of retail breaches out there, it makes a lot of sense that they're engaged with us. And then healthcare organizations. I think what you'll notice about these type of industries is that they're actually ultra-conservative. And so regardless of the fact that we're doing something pretty progressively leaning, we're finding that these organizations are opening their arms to this idea and embracing the idea of crowdsourcing and recognizing the only way they can get ahead of this cybersecurity issue is by using things that are innovative, and using things that are outside the box, because frankly the old stuff is just not working. Just recently we announced two large contracts with two federal customers, one the Internal Revenue Service, we've all seen the news of the IRS being breached, so it's great to see them taking more of this progressively leaning view on things, as well as the Department of Defense arguably one of the most conservative organizations in the world saying we're getting attacked too much, the attackers are winning, the only way we can defend against this stuff is by adopting a solution that mimics those same attackers that are attacking us. This is something we didn't expect and I think it's really cool and you know when we started the company is was all about we're going to try to bring as much revenue into the company, we're going to try to sell to as many customers as we possibly can, but what we didn't realize was that the people that we were leveraging all over the world, in countries like in India, and Russia, and Eastern Europe, they're actually starving people out there that are really good at this work. They have computers, maybe they go to an Internet cafe, they love just breaking things, they have the hacker mentality the hacker mindset. And we started putting food on their tables at home. And I think that's really exciting, we never thought that that would be possible we thought hackers that we would be employing would all be experts, they already were making a lot of money. And we we're going to provide them much more benefit than making them richer I guess.

But I absolutely love this quote... SRT stands for Synack Red Team, and that's what we call our community of hackers, so one of our SRT members wrote in and told us what we're doing for him. So I want to end with just some learnings. My key entrepreneurial learnings, Tina asked me to throw together some things that maybe you can learn from. A lot of this I already talked about. But I think starting off, don't just write a trend, build a lasting company, it's one thing to say I'm going to do cybersecurity in a crowdsourced way. It's another to actually build a company that addresses all the problems associated with selling to businesses, selling to conservative enterprises, in cybersecurity and crowdsourcing at the same time. So that was definitely something that we learned was really important. Surround yourself with the right people, we talked about that hiring really top-notch talent, bringing on great investors, advisors, mentors, super crucial. They have really propelled our business forward and got us to where we are today.

Conviction, you got to stay the course even if people call you crazy, they will call you crazy, if they're not calling you crazy, your idea probably is just boring. So do something that's exciting, people should call you crazy and then you should figure out how to prove them wrong. Be passionate, but patient about the grand vision. It takes time, it takes time to build a business. I'd say the last year, we've been at this for about three and a half years, the last year or so we've really hit our stride with respect to bringing on new customers at large contract values. Our federal customers are new, we've been going after them for quite some time, enterprise sales takes a really long time you have to not only convince customers, but you have to get procurement process, that's really hard. They're very conservative with dealing with smaller companies, but they're starting to embrace it more and more. And then execution, it's one thing to start a company and it's another to actually execute. And sorry this is so small by the way, I see some of you squinting. But really at the end of the day it's all about execution and executing on that early idea that you had to make it a reality.

So with that, I'll take out questions. (audience applause) I'm going to go to that side. - [Audience Member] Can I ask the first question? - Maybe. - [Audience Member] Okay, may I, thank you. I would like you to explain a little bit about the hacker mentality, the black hats versus the white hats. What motivates people to break things and break things for good versus break things for evil? - It's a great question, so the question was talk about the hacker mentality, what makes a hacker a black hat versus a white hat, black hat being someone that's hacking for bad purposes, the white hat are the type of people that we

employ. And I guess what ultimately makes them want to hack in the first place right? You know it's a great question. We have people in our community that come from a variety of different backgrounds, they're developers, they're people working for big tech companies, they're people working back in the government space, some of them are trained, some of them are just really good at this and they figure it out at an early age, that's kind of how I learned. Just trying to break things and take computers apart and figure out how to bypass authentication and do all kinds of interesting stuff. So I mean what makes a hacker a black hat versus a white hat, well I think some people are certainly attracted to the money on the black hat side.

There's actually a thriving market as it relates to selling exploits on the black market as it relates to hacking banks for example and trying to steal money. But the reality is, before there was not really a legal mechanism for them to operate, especially if they were just sitting at home and so our hope and our goal is to actually turn these black hats, or people who are thinking about going more the black hat route, and telling them hey you can actually make money doing this legally. You can still set at home, sit on your computer, but we're going to make you money hacking our customers, obviously we're going to make you sign a lot of agreements saying you're never going to talk about this outside. If you find something we're going to need to monitor your traffic and so forth, we need to know that we can trust them. But I think the reality is you're starting to see a big shift and I would say the black hat market isn't as massive as you would expect there's a lot of people doing this for good, and so is people we're ultimately going after. But I think you're going to see a shift. There's always going to be money on the other side. But that's definitely starting to shift the other direction. Yes. (audience member mumbles) So the question was, what do we do to build our community of hackers? So we early on recruited a lot of people that we knew in our network, we were pretty well connected, we just pulled a lot of people off from government.

We went to a lot of security conferences and we would basically set up a booth and we'd say come join our community, there's some very large hacker conferences in Las Vegas, one's called Black Hat, another is called Defcon so those were prime examples. Sooner or later hackers started hearing about this and they realized wow, there's this company I could just work for on the side, I can still keep my day job but I can do this work nights and weekends. And we started to get a lot of inbound interest and so we created a whole application process around that. We now get quite a few applications, most of our researchers come inbound at this point, we then put them through our assessment process and vetting process and then ultimately pass them through, but we continue to recruit at events. We continue to put out incentives for people to refer their friends though it's a little bit harder than you would think because by referring their friends they're actually creating competition for themselves. We have a whole leader board system, we have a whole system where our hackers, the first to find an issue is actually the one to get paid so by bringing additional people in, you're creating competition. And so referrals doesn't work quite as well as you would think, but there's a lot of different areas that we're recruiting in and obviously a lot of that's inbound at this point. Yes. - [Audience Member] Do you when you're working with potential clients, do a test run to see if they are vulnerable and if they're not have ever signed with a client and had to say sorry we couldn't find any vulnerabilities. - So the question was do you ever test a client ahead of time to see if they're actually vulnerable, then tell them to pay us and then not actually find anything and just say sorry.

It's never happened before where we haven't found a vulnerability, never happened. From the entire time we started the business it's never happened, with that said, you certainly get to a point, 'cause our customers sign on subscriptions, so they're constantly engaged with us. And there becomes a point where they're getting pretty robust from a security posture perspective and we're not finding as many issues as we used to. And the way we prove value to those customers over time because we want them to stay on as a customer, year two, year three, year four, is by showing them activity and actually showing them we're still trying. And showing them your applications are changing, so we need to keep looking because you could be introducing a security issue at any point in time, your infrastructure is changing all the time, we need to keep looking as well. And so we prove value in two ways, one is obviously finding vulnerabilities and helping them fix them. But the other of course is showing that we're trying and we're not successful and that's a great metric for anyone that's a security executive, 'cause they're all trying to prove that they are getting better and they're doing a good job and so we're able to help them at least quantify the fact that things are getting better over time. Yes. - [Audience Member] So you talked about scaling by adding technology can you talk about that? What kind of things are you doing to essentially put these hackers out of business? - Yeah, so the question was can you talk more about the technology side, how that helps us scale the business. So the reality is we're never going to be able to cut the hackers out entirely.

There's an entire class of vulnerabilities that you simply cannot replicate using technology, you can't automate. If you think about an online banking application for example a piece of technology or automation sees a bunch of form fields on a website, it doesn't have any clue what those form fields are but it's going to send a bunch of data to those form fields, it's going to hit the Submit button and it's going to see what it comes back. And it's going to see does it match any signatures that are built in to the automation. A real person sees, okay there's one account here, there's another account here, then there's a transfer button if I'm able to transfer money from one account to another and I'm not the owner of that originating account that's actually a really bad thing. And those business logic abuse cases, that's one example of why you can't cut out the hackers entirely. But there are also a slew of vulnerabilities that you can automate, you can actually build technology that finds this stuff more programmatically. And so for that low hanging fruit, we're definitely going to be concentrating on building the technology but

we're going to try to level up the game for the hackers on the other side so they're focused on the issues that we want them to focus on which are the things that we can actually automate. And that's how we're going to scale the business long term. We hope the automation becomes more and more robust to the point where we aren't as heavily reliant on the researcher community as we are today. And we're definitely moving in that direction.

Yes. - [Audience Member] What measure do you have in place to make sure that your researchers do not fail the system meaning that either they themselves or their friends create a problem first and they get paid by you to fix it? - Okay, so the question was what stops researchers from gaming the system, so I guess potentially paying I don't know a developer to put a bug in so that they could find it and then ultimately report it and get paid. You know I think there's a lot of ethics that are tied to our business model, it's part of that trust process when we put researchers through vetting just to get a sense as to what kind of people they are. Certainly if they're working for an organization that we're doing business with, they're not allowed to participate on those projects, so it at least gets rid of that scenario. But I think a business unit owner will start to ask questions if they start seeing the same developer bringing the same vulnerabilities into a code base over and over again, that will definitely raise questions. And at the same time, it's an interesting question, we've never seen it before, I guess theoretically it's possible but I think it's pretty unlikely. Yes. - [Audience Member] So you were talking about leader boards have you implemented on the other stuff, towards (mumbles). I could guess that your hackers are triggered by some form of gamification. - Yep, so the question was around gamification and leader boards, I mentioned that we built leader boards and as a result we've gamified some of the platform.

Yes, gamification's really important with this community hackers are not necessarily only working because they want to make money, they actually really like the notoriety they really like to be seen as a top-notch hacker in the community and so we've created those leader boards for that purpose, they're welcome to advertise that wherever they want. Some of them put it on their Linkedin, some of them put it on their business cards, we've seen cases where they advertised that all over the place. It actually is pretty meaningful to be part of our researcher community to begin with, we only accept about 10% of the folks that apply and so it's pretty rigorous from that perspective, but even further, being a top-ranked researcher with Synack is pretty meaningful. And so that's what we have today from just a gamification perspective. We do utilize points on the leader boards for prizes as well so we basically will send hackers to conferences, send them different swag and all kinds of stuff depending on where they rank. So there are a bunch of things that we do with that, but I think it's the notoriety that plays the biggest role in keeping them motivated. Yeah, full of questions. - [Audience Member] I am, always, very curious. So you talked about gamification which is super interesting I'm fascinated with the culture more broadly of the company what kind of culture is there in the business and what kind of levers do you use to influence it? - So the question was about culture in the actual business and what do we use to influence the culture. When we started the company I said I want to create a culture that's a complete 180 from the federal government look we're working on really cool projects, it's exciting, saving lives, but at the end of the day there's a lot of bureaucracy and it's hard to get things done if you have a really brilliant idea it has to go up many levels of chains and management and sometimes you have to really beg for money and you would think wow, but you're working intelligence it's like counter-terrorism why are people ramification's you a hard time, it's not as easy as you would think.

In the government you also have to basically pay for every little thing if you want a candy bar, you got to put it in the jar, people can't give you free stuff. We wanted to cut all that nonsense out and we really created the typical Silicon Valley culture out here. But for people that are interested in cybersecurity and we actually pull a lot of people out of the government in there, they're like wow this is amazing. And so we have a very non-bureaucratic system at Synack. If you come up with a great idea we empower you to work on it, we never want people to be bothered or burdened with paying for a candy bar, we give them as many snacks and drinks as they want, I'm sure you guys have seen the startups in the Valley and what it's like. But we almost use the government as a guide of what not to do. And then win with the opposite. Not everything's so bad especially where we worked, it's a pretty laid back organization, you wear jeans and a t-shirt and people are pretty geeky and nerdy at the NSA, it's not like in a lot of other agencies. I worked for another couple DOD agencies and it's very different there, suit and tie kind of thing. But yeah we sought to create a very different culture than we were before.

Yes. - [Audience Member] So you mentioned that you really enjoyed your job at the NSA so why did you decide to leave? - So the question was since I really enjoyed my job at the NSA why did I leave. And it's a great question it's one that I grappled with for a while, I thought about I really love what I'm doing, counter-terrorism is such an exciting mission. But at the end of the day, I was an entrepreneur at heart, I really wanted to build something I wanted to start a company. Actually backing up, I started a company when I was like 13 years old I built a web-hosting and development company and days before Amazon, AWS, and Microsoft Azure and Google Cloud and it was basically a shared web-hosting business, put a bunch of servers online, rented space out, built it to over 1000 clients and then I ended up selling it. So I really enjoyed that, that was a lot of fun for me. It was obviously nothing like the business that I'm building right now, but the reality was I did not see myself being a career government guy, and I knew I wanted to start something, I just didn't know when timing-wise when I'd be able to, but I decided to dive right in and just make it happen. People think the government's losing all this talent there's such a talent problem, the way I look at it is they're able to get really great talent even for four or five years and that's not necessarily a bad thing. You're pulling people out of college, you have these great scholarship programs like the one that I went through. And

being able to leverage them on even just a shorter-term basis it's not terrible.

And so I encourage anyone who's thinking about entering federal service it's not necessarily a life-long project. You can go in, you can learn a lot, you get exposed to really interesting things, really interesting people, and obviously the stakes are really high. And then you can earn that credibility to go do whatever you want to do. - [Audience Member] So isn't there a place for entrepreneurship in the government? - Is there a place for entrepreneurship in the government? There is and I think the government's being a little better about it today more than they ever have. There's a lot of new organizations that are spinning off that are trying to bring Silicon Valley companies into the federal government, you're seeing the DOD recently launch something called DIUX, it's the Defense something Experimental Unit. And the whole point of it is to basically take innovation from outside and bring it in and generally it's more of the entrepreneurial thought leaders within the federal government that are spearheading those initiatives. And so I think there's a lot of opportunity in the federal government to innovate, to be entrepreneurial, to build things that are exciting. I mean even my job I think while I complain that there's a lot of bureaucracy, we did have a lot of freedom and we were able to think really creatively because the projects that we were focused on were, how do we gain this intelligence from a potential terrorist and we had to take all of this data, we had to talk to analysts from all different buildings and bring it all together and it was a huge group effort. And I would say a lot of the same things that you would do building a company you can do in the government it just looks different. Your end product is not necessarily a company or a product or a piece of software, it ends up looking more like I just stopped a terrorist attack, which I think is just as exciting.

- [Audience Member] Well thank you for your service first of all and congratulations on all your success. Please join me in welcoming Jay. - Thank you, thank you so much guys. (audience applause)