***Barclay Damon Live* Presents *Cyber Sip*™**
Season 3, Episode 14: "The CrowdStrike Incident: What Happened, and What Can We Learn?"
With Brian Haugli
Host: **Kevin Szczepanski**, Barclay Damon

[Kevin Szczepanski]: Brian Haugli, CEO of SideChannel, is back with us to talk about all this flak over CrowdStrike. What happened? What does it all mean? And what, if anything, can we learn from it at this early stage? Brian, welcome back to *Cyber Sip*.

[Brian Haugli]: Hey, thanks for having me on ...

[Kevin]: ..and I'm grateful you were you're in transit today and you stopped back to the studio just to join us. So thank you very much.

[Brian]: No. No worries. It's easy. It's, they both happened to be where my house is, so...

[Kevin]: I much appreciate it. All right, so let's start with the basics, because I think a lot of people know, but a lot of people don't. What is CrowdStrike? What do they do?

[Brian]: So in the simplest terms, they're what's known as an EDR or a "endpoint detection and response" capability. So in the days of old, antivirus used to just kind of block and stop things from happening, right. EDR was the paradigm shift for everyone to go from, "we can stop it" to "stuff's probably going to get through." So if it does get through, how do we make sure we can detect and respond to it? So it's an agent, like a piece of software that goes out on every laptop or server in a corporate environment. And from there, back-end system is able to then use to see what's going on inside of, you know, each of those systems is, you know, what processes are running, what applications have started, what files maybe have been created, what connections are being called out to, you know, the internet or things like that. All of that is used to essentially determine is something bad happening on that server, that laptop.

[Kevin]: So this is kind of a left field question, but I think it sets the table. How big is CrowdStrike compared to its competitors? Who are its competitors? And I think we'll come back to that later when we talk about the impact of what happened.

[Brian]: Yeah. So CrowdStrike's right now, in my view, from everything else I've read, they're the largest... they probably have the largest market share as an EDR provider. Right behind them, you've got the major competitors are SentinelOne. And then actually Microsoft's Defender solution as well. I kind of put those three in kind of a tier one category, right. Biggest, you know, best of class, upper right-hand quadrant if you follow that sort of thing, the next tier, you've got other EDR providers, you know, out there, you know, things like Field Effect, they have their own solution, own platform, trying to, and solving for the same thing, probably a little bit more cost effective. So you've got other providers that are out there, then you've got kind of this new wave group of new tech startups that are trying to build the better version of EDR. But really, right now, you know, CrowdStrike has the, I think the largest market share, as far as EDR go. I think the, what we're going to talk about today and actually out of the incident, the numbers that came back, they had about 8.5% of all Microsoft systems worldwide was where they were...

[Kevin]: That's a massive number.

[Brian]: Massive number. Yeah.

[Kevin]: All right. So Brian, let me take you back to Friday, July 19. What happened to cause all these stories we're hearing about today?

[Brian]: You know, it's, it's unfortunate what happened because, and it was an update, right? We know and we see it all the time on our on our laptops, on our systems. We begrudgingly see, hey, I have to restart because an update was applied or, you know, it has come forward and told, you know, the workforce, wherever you are. Hey, we have a maintenance window, or we have to patch all the systems and we're going to have to force reboot your computer. But those are all generally associated with some type of software update. And what happened on that morning was CrowdStrike pushed an update. What's interesting is how they did it, how it was actually kind of rolled out. And what the impact was obviously was a negative impact.

[Kevin]: Sure.

[Brian]: So let's kind of like walk through like what you're supposed to do is that that kind of okay, Kev?

[Kevin]: Let's start there.

[Brian]: So, so generally when you have some software, right, whatever your software is, right, you have an application, okay. You're going to build that application. It's going to have a number of different components inside of it. And each of these components need care and feeding eventually at some point. Right. At some point, you know, this is number one, like this component. Somebody might find a vulnerability in it. Somebody might... there might be a new feature that is required. And it's not always bad. Right. It's not, you know, because there's a vulnerability. But maybe we have a new feature that we want to deploy. And the only way you're going to get that new feature is if we update the software or, you know, here maybe this component actually there's a vulnerability found in that software. So we have to update it from version 2.3, it needs to move to 2.4. I mean you kind of see this happen all the time. So there's always good and bad reasons why you have to update stuff. So that's kind of the reason, like, why do you have to update? Well the process that you want to update things is, is actually kind of pretty straightforward. You essentially want to test your software. So you have the provider that makes the software. They're going to release a patch. Right. And that patch is going to go out to the entire customer base. That customer base is going to ideally take that patch and put it into a test pool. Right. Maybe just a handful of systems, maybe some systems that people don't even use. They're test servers over here on the right. So worst case scenario happens, this patch gets put on to a test environment. Nobody's really impacted. Right. And then, you know, ideally you then test on a smaller pool of production users. Right? Especially if it's like an end-user. So we're updating Windows 10 or Windows 11. You're going to do a small test of non-user laptops, and then you're going to find some willing guinea pigs generally maybe it's the IT team themself. They're going to test it on their own systems. Right. So you're going to have a small pool, right. And then eventually you're going to say okay the, you know the patch worked. It worked in test. It worked in the small pool. Now we're going to roll it out to a larger pool. And then we're eventually just going to roll it out to everybody. So there's steps right. And all along the way you're checking to make sure you're not you have an adverse impact. Right. CrowdStrike didn't do that. CrowdStrike, what they did was they released the patch directly into all customer's product, the Falcon product, that was deployed on wherever, wherever they were installed. So they basically did—and skipped all of these things on behalf of all the companies and all of their customers.

[Kevin]: Can I just stop you there, Brian? What is it? Is this CrowdStrike? As we said, large market share, this is a sophisticated EDR firm. What would possess a company in that position to skip those critical steps? Is it overconfidence, is it a question of timing? Is there something else? Is it, as you explain it, it makes no sense at all. Well, the way you're explaining it makes perfect sense. It makes no sense that CrowdStrike would have done it the way they would have done it.

[Brian]: Yeah, honestly, I wish I knew that answer. And I think that's the biggest question that everybody has. And while the postmortem is happening and you've got all of these, you know, responses coming from CrowdStrike about what they did or didn't do or how they came up with it, you really got to kind of wonder, you know, how much of that can you trust, given that they just did this? But, you know, I don't want to get myself into, you know, like a libelous position.

[Kevin]: We don't want to cast aspersions. Yeah.

[Brian]: This is, this is just my opinion. When you… when you're kind of king, you know, when you're when you're sitting in… the crown is heavy, right? And you're kind of at the top. You got to, you got to move fast on certain things. I think they've also got a protective mindset where they're thinking, hey, we got to protect our client base. And that's right. That's good. So we're doing this on in their best interests, right? We've got to move fast based on what we're seeing that's out there right. I think they had, you know, best intentions. And what I think, unfortunately, it worked against them is a real lack of rigor around their own QA, their customer… kind of connection to what customers are expecting to be able to do within their own QA. And I think maybe they just they just got a little in over their skis. And made a deployment. Look, we… this is not unheard of that updates have done this. Microsoft has done this to their own operating systems. You know, other platforms and software have done this to their own, systems and platforms. It's not unheard of. What's interesting is this is really the… I think one of the first true cybersecurity products, which is, which is built to protect you, that is now because of an update, hurt you. So, you know, there's got to be some… I think there's going to be some lessons learned here about vendor selection. What we're going to allow vendors to do. What's in our procurement contracts that we're going to hold vendors responsible when they…when and if they mess up. Yeah, I think there's a lot of really interesting things are actually going to help customers better think about application security, application software development updates, and things like this, and even just vendor selection kind of going forward.

[Kevin]: No, that makes sense. And we're going to come back to that in a moment. But let's keep tracking this through. So you've explained it very well. It makes sense to me. So you must have explained it well. All right. So they're trying to roll out a patch to their EDR. It goes wrong. How is it discovered and what does CrowdStrike do in response? Because that's part of what you were alluding to earlier. And I think you've mentioned a couple of times, it's sometimes not what happens. It's how you respond to what happens when you're in CrowdStrike's position. And if you respond well, your clients may ultimately be happy. But if you respond badly, they're going to be even more upset and write some of the nastygrams that we're going to talk about later. So I don't know if that question was very long and convoluted. So let me, restated, what did they do when they discovered the problem?

[Brian]: I think it's interesting that they didn't discover what they did. They were told what they did. Right. So their customer base very early on that Friday morning, I go by East Coast time. You know, Europe had it happen much earlier than the US, right? You know, following the sun. So you had this impact happening and the impact was it was not just like, oh, there's an error. Please come back and fix this later. No, this error was full-on system reboot/blue screen, which means that server system never boots up to the operating system. It is essentially crashed. Any applications or services that you're running on there, whether it's your e-commerce platform, a customer portal, an internal portal, website, whatever it is you're running on, those systems were down. That's actually not hitting CrowdStrike. CrowdStrike is not knowledgeable about that. That's hitting every customer of CrowdStrike. So every company out there is going, oh, our entire Windows/

Microsoft environment just went down. What happened, right? So initially you've got in the first hours of triage, you've got, okay, is this an incident? Is this, is this an application. Is this an operating piece? Is this ransomware like, what's going on? So you've got for the first time just people trying to figure it out. And then obviously the message boards, people start kind of sharing information. Hey, it was this... it was this update. Here's what it is. Here's where it is. And then it was hours until CrowdStrike actually came out and said, here's the fix. Right. And I think the way that they kind of said it was, you know, here's the fix. What I think was... it kind off on the response was two things that I saw. One was a post, and I forget where because it got kind of copied a couple places. But George Kurtz, who's the CEO of CrowdStrike and then also I believe their president of CrowdStrike, both came out and basically said, hey, this happened. But there wasn't this overwhelming sense of like, we are sorry that this happened to you. We're sorry we did this. It was much of just like your customers think forward, we'll get through this blah, blah blah.

[Kevin]: And you're like, that's easy for you to say. Yeah, right.

[Brian]: I'm sorry. If I'm the CEO of Delta right. Yeah I'm sitting there going...

[Kevin]: I've just canceled 2,000 flights. Yeah. I'll go up and fly. Right is not going to...

[Brian]: Yeah I'm about to have the secretary of transport on me because we have new rules about flying. You've got, you had a lot of major corporations that were down, and I just don't feel like, you know what I saw. And again, I don't work for CrowdStrike. I wasn't impacted by it, honestly. We actually were big proponents of their number one competitor, SentinelOne. For a variety of reasons. This actually QA and culture of the company is one of them. So none of our clients were really impacted by this, save a few that, you know, we... they had already been using it and we just didn't position it to them as a, as an EDR. But I think now they're generally reconsidering it. So I was an impact. I this was one of those events where I sat on the sideline and just read and watched everything, and I felt, you know, like a, like a really unbiased view of just like I have no stake in either and how this is going. But this is interesting how it's playing out. And it just it did seem like it lacked, I don't know what the right word is...

[Kevin]: "Bedside manner"?

[Brian]: That's a probably that's probably a good way to look at it. Yeah. Like. Thank you. I know what happened. My arm is broken, but you could have, you know, told me that, you know, how this was going to go about a little bit better so I didn't feel so bad. Right, because I maybe. Yeah.

[Kevin]: Anyway, it's interesting you say that, Brian, because I remember years ago reading, I don't know if it's the CEO or the president of Target writing to customers when the HVAC vendor was hacked, and that led to the huge Target breach. And I don't know, I don't remember exactly with the letter said. But I remember my response to it, and it was sort of like, wow, this is really stiff. It's not unfriendly, but it's not terribly friendly. And I felt like it was a missed opportunity and maybe worse than that, sort of what you're talking about. It's not just a missed opportunity, it's "you're starting off on the wrong foot with your first communication to the customer." And when you do that, it can be very difficult to get back on the right foot.

[Brian]: Yeah, but you've got you have genuine companies out there, midsize and enterprise companies out there that CISOs are heavily weighing, do I stay with this product? Yeah. You could chalk it up with they're never going to do this again and make sure that they never do this again. But what inside of their culture and their engineering allowed them to even... allowed this to happen in the first place? How much of that can you actually expect to change in an organization? Right. And I'll be honest, I haven't seen any major changes inside of CrowdStrike announced, where that would make me believe that culturally and from an engineering standpoint, they're making, you know, some moves to do that. So there's no signals that are telling me that they're changing anything inside to make sure that doesn't happen again. And it seems like it's like, okay, we learned from this, we'll get over it. We'll move on. I mean, I'm not saying heads need to roll, but, you know, they're a publicly traded company, right? I'm sure the board is having some very interesting conversations with the C-suite about what just happened. What did you just do to... like, they've lost a significant, you know, market cap because of that event. It was interesting to just see it go... right, because of what they did. Now will be the tale of what continues to go on. Are there lawsuits? Are there any other things? Is the SEC going to look into this? I mean, I was actually kind of shocked to see that CrowdStrike itself filed an 8-K about this. I was like, I was actually I was scratching my head. It's like based on the SEC rules, would this have been considered a cyber security incident that CrowdStrike or a publicly traded company would have had to have filed for?

[Kevin]: Interesting.

[Brian]: Yeah. I'm still kind of trying to figure that one out.

[Kevin]: I mean, one of the one of the touchstones is the materiality of the effect on operations. And one would think from reading the Delta letter to CrowdStrike that Delta would have filed an appropriate disclosure as well, because by all accounts, they consider it to be a significant, as having had a significant effect. Before we continue, I just want to pivot back to one technical question or two. As far as we know today, the problem has been fixed, correct? In other words, they... CrowdStrike was able to roll out a fix for the flaw in its initial fix, its initial update. And as far as we know today, that has been remedied.

[Brian]: Yeah, they published a how to... on exactly what steps need to take place to be able to undo what had been done. And I believe since, you know, other updates have been pushed out to the agents and been released in a way that have been consistent with, you know, traditional practices of testing before deploying to production. So by all accounts, right now, they, you know, they're back to normal operations, normal updates, normally taking care of their customers, from, from a technical standpoint. Correct.

[Kevin]: You have to give credit where credit is due. It was a massive failure. But it was rectified relatively quickly. And we will see in the coming weeks and months how many corporations come forward with claims. Delta made public a letter to CrowdStrike alleging half a billion dollars of damages. And today—we're recording this in early August—we've seen CrowdStrike's response, saying, well, we're disappointed that you felt the need to do that so publicly. We actually think your damages are a fraction of that. All of that is going to play out. One question I have for you, and you can take this anywhere you like, Brian. But if you're a business that's using the CrowdStrike platform today—and I appreciate this is not something that you or your clients do—if you're using the CrowdStrike platform today, what should you be doing to evaluate to assess risk? I appreciate that it's perhaps outside the hands of many of these companies because they're relying on CrowdStrike as a vendor, but what should those companies using CrowdStrike be doing today to manage the risk that this might happen again?

[Brian]: Yeah. Well, I you know, I'll say this. I don't believe this is like a knee jerk reaction time for anybody. Right. Let's also just kind of back up and remember, what is it that this product is supposed to do. As a cyber security professional, I want to see more companies embracing using EDR technology. You wouldn't believe how many don't, right? Bad guys will get in. How you detect and respond to them will set you apart from those who don't detect and respond. So I really hope that there's not this knee jerk reaction to just rip this out and not do anything and replace it. Or be hesitant in applying good practices like rolling out EDR solutions to your fleet or even handling updates. I think that's what I think the big conversation that I've had with other professionals is, oh, I really hope that CTOs, CIOs don't go and say, okay, well see, see an update, see what the update did? Like, we can't do updates now or we have to take all this time. No. We just need to follow good processes about updates. We don't need to abandon doing updates. Vulnerable software exists. It will continue to exist as long as people keep making software. So abandoning you know this just because of this incident is the wrong way to go. So again, I really hope that everybody at large does not kind of take this knee jerk reaction to, hey, we obviously don't need this. We'd be better off if we didn't. Actually, I don't think you would. Yes, this thing happened. Unfortunate. Hopefully it never happens again. Other vendors out there will probably not let this happen. But do not abandon all the good security practices that professionals have been talking about for years and really trying to move the needle. I think kind of, you know, next steps as far as what folks are going to do, I think they're really going to dig into procurement language. Technical process, I like I outlined it right here. It's pretty straightforward. You get it. You test a little, you test a little more, then you roll it out. It's pretty straightforward. It there's a lot more to it. You know I like how you do it. And when you do it and but like that's basically the process. I think the part that gets missed is when you bought that product from that vendor or that reseller, what exactly are your responsibilities, their responsibilities? What are you allowed to do? What are they allowed to do? I don't think enough security professionals actually dig into that side, because generally you kind of have you know, cyber... and the CISOs sitting here and then you've got procurement sitting over here. Right. And there's this I need, you know, I need a contract. And it's back and forth. I think there needs to be a little bit deeper of, of an understanding of I need this software. Okay. This software is... uses this contract. Can we just be a little bit more of a team to better understand what this is, get procurement to fight with the vendor a little bit more about, you know, the Ts and Cs. Really understanding as a CISO or as a security professional, if you're not large enough to have a CISO, what is it that the vendor's on the hook for? Because I've heard some stories about people who have actually dug into their CrowdStrike contracts and what, what CrowdStrike is going to basically say, well, we're not responsible for these things here, here, and here, because that's what's in the agreement, you know? So fighting for better Ts and Cs, fighting for better control so that the vendor just can't update things carte blanche, unchecked in your environment, things like that. The ability to audit, the ability to kind of dig in a little deeper. And then, honestly, maybe an honest look at alternative, you know, vendor solutions. Did most CISOs or people who, you know, are in charge of these programs, did they buy this product just because it happened to be in the upper right quadrant and had market share? Because their buddy used it? Because they used it at their last place. How do you know that it works for you. Your environment. There's nothing... another selection that's out there. I don't think it's always just technical requirements that we need to judge a product on. What do you need to understand that. Yeah a lot of other things. So there's a lot that can be done and should be done. And I get it. Not everybody has all the time. But these are the types of things to start kind of thinking about when you're responsible for the security of an organization.

[Kevin]: No, I agree, I really want to embrace that point. And I would add, counsel, you have your... so you have your CISO, your procurement, and also you're in-house and, and if you need be, outside counsel, because you want to make sure that those contracts are... you want to you want to look at those contracts from a technical aspect. You want to look at them from a legal aspect, an electronic aspect. All of those forces need to be brought to bear, and it really doesn't...if you integrate everyone at the right time, it really doesn't have to take much longer. The problem comes when you may have in-house CISO and procurement. Get to the 11th hour, and then you turn it over to the general counsel and say, we need you to review and approve that. That time. It's going to be very difficult for your GC to notice and tweak the potential issues in that contract. And I think you're absolutely right. We saw CrowdStrike response to Delta's $500 billion claim. And I'm sure part of that response was, well, let's dig into the contract because as I think you'll see, we've limited our liability contractually and going forward, that may not be for everyone of CrowdStrike's customers. So I know we're getting the end of our time. One last question, Brian. You know, when things like this happen, some of us think of, what if this were systemic, what if this were a cyber warfare attack? What if it were something even more serious? Is there a role for the government to play in looking, peeking under the tent of companies like CrowdStrike? I've heard people talk about stress testing EDR firms in the same way that, the federal laws require banks and other financial institutions to be stress-tested. Do you see anything like that coming along? And if... you does, it makes sense.

[Brian]: Well, I'm kind of a small government guy when it comes to it. I'm heavier on states' rights versus federal, kind of oversight. But I do believe where, you know, the states can't collectively come up with something, that's where you need the federal government to step in to, to do what's right. It's interesting, you know, is EDR and cybersecurity as a, as a industry, would that be alone considered critical infrastructure. Right. So if so okay. Like do we have a horizontal responsibility across all of the 16 sectors that DHS has to make sure that that’s right. Well, I mean, maybe power right is required by all 16 and power alone is a, critical infrastructure dubbed by the DHS, maybe cyber security is right. I think if we look at this as a national security, concern, then. Yes, evident. Like it’s an obvious... anything that we’re doing to protect corporations and companies. Yes, that that’s evident. But if we don’t look at what that is as a national security concern, I don’t think the federal government does have a role. Could they maybe apply, known as “s bomb” like software, build materials and, and process kind of controls into regulation? They definitely could I mean, I think there’s plenty of precedent in other regulations where they’ve looked at not just, you know, the technology, but the processes to create technology or create assets. So the government could definitely step in there. So, yeah, I think it’s going to depend on like, how does the government look at that? I’ll be honest. And anything I’ve seen out of the federal government, out of that since, you know, I left DoD in 2015, even then through then, their part in regulation and applying pressure through regulation on US companies is not their strong suit. So if they’re going to do it, they got to figure out really how to do it right. I just don’t think they’re in a position, honestly, at this point, to be able to do it right. There’s going to be a lot that has to go into that. CSA is not in a position, in my opinion, where they could step in. Because they would be the probably the most obvious choice or arm of the government to do this. They’re not in any position today to be able to make that happen across companies at large. So yeah, unfortunately, I just don’t think we’re mature enough as a federal space, understanding cyber security and its impact, to be able to effectively have a program to do what you’re asking, right.

[Kevin]: Or fortunately, we we’re not in that position. I think what’s going to happen is this is likely to fall under the rubric of vendor management. So if you have an arrangement with CrowdStrike and they’re handling your EDR and something goes wrong, you should expect as a business that if you suffer some ill, your customers suffer some ill, as a result, regulators are going to be looking to you and asking you the question and how you vetted your vendor, even a vendor of the size and scope of CrowdStrike. Sure. Yeah. All right. Well, Brian, we have to leave it there. But thank you so much. Really appreciate it. This was a very insightful discussion. I think we’re going to see more. We’re going to see more claims. We’re going to see clamoring for government oversight. And it’ll be interesting to see how it all shakes out.

[Brian]: It definitely will I agree. Thanks, Kevin, I appreciate it. I appreciate it.

[Kevin]: So thanks to Brian Haugli, CEO of SideChannel.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied.

Barclay Damon Live *podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of Barclay Damon Live programming is the audio file. Thanks for listening.*