



Barclay Damon Live Presents Cyber Sip™
**Season 4, Episode 1: “Your Laptop Goes Missing!
What Do You Do?”**

Host: Kevin Szczepanski, Barclay Damon

[Kevin Szczepanski]: Hey, everyone. Welcome back to *Barclay Damon Live’s Cyber Sip*. I’m Kevin Szczepanski, and we are now in Season 4. If you had told me four years ago we would do four seasons of *Cyber Sip*, I would have been surprised, but I’m not surprised now. In fact, I am grateful to you and so many others who have helped make this possible. You join us every week, you give us your likes and your feedback, and we have a great team internally at Barclay Damon, led by our managing partner, Connie Cahill, who’s been so supportive, and also our head of marketing, Maureen Fyke, and our fearless producer, Kyla Handley, who’s watching this now and hopefully making it a lot better than it looks to me, because she’s fantastic and can do that.

[Kevin]: But anyway, welcome to Season 4. Today I want to start by telling you a story, and it’s an embarrassing story. I thought long and hard about sharing this because it will reveal my carelessness, but I think it’s important because people like me make these mistakes every day. And maybe if I share my story, it will make you and yours safer. So the story begins on December 5, and I am at the George H.W. Bush Airport in Houston. And unlike my hometown, Buffalo, New York, where our *Cyber Sip* studios are, in Houston, you have to take... you still have to take your laptop out of your briefcase and put it in one of those bins so that it can be inspected separately. And I wasn’t prepared for this, because on the flight from Buffalo to Houston, I didn’t have to take out my laptop. So here I am in Houston. I just made it into the airport in time, kind of rushing through security, and I realized that I have to take my laptop out. So I’m juggling my laptop. I pull it out, I put it in its own storage bin, and I take off my shoes, walk through security, and on the other end of security, I get another distraction because I have been handpicked to go through the expedited screening, which was a very personal screening. By the way, I kind of felt like I was in prison. But anyway... I say that to you because that distracted me as well. So I went through the personal screening, I turned around, and I saw my laptop, Dell laptop. It’s the very one I’m recording this session on today, and I picked it up. I put it in my briefcase, packed up the rest of my stuff, my shoes and my coat in my arms, and make my way out of the security lane because I can’t wait to get out of there, frankly.

[Kevin]: So it’s pretty quiet at the airport. Long delay. I didn’t get back until after one o’clock in the morning. I didn’t get to sleep until around 2. And so the next morning, I decide, you know what? I’m going to sleep in for an hour or so. I get up. I don’t know when I get up, but I was sitting finally at my desk at around 10:00, so a little bit of a late start; hadn’t yet opened up my laptop. And I never did, because I start getting phone calls. I get a phone call from one of our veteran legal assistants saying, “Mr. ...” And I’m going to call him by an anonymous name. Although he turns out to be a hero. “Mr. Smith is calling you. He has an important message for you.” And I thought, okay. And I’m getting myself sorted, ready to return the call. I get a call from my own assistant telling me, “Mr. Smith called you, it’s a very important message.” And so I said, okay, I need to log on and get going. And I picked my laptop out of my briefcase, and I open it up and I realize it’s not my laptop. So I figure out that maybe this Mr. Smith is calling about this problem I’ve just discovered: I have lost my laptop. The last time I used it was in the office where I was earlier, yesterday in Houston. I didn’t use it at the



airport. So I'm realizing now, for the first time, that... must have been in the TSA line that I picked up someone else's laptop that looked identical to mine. So sure enough, Mr. Smith is trying to reach me.

[Kevin]: I call "Mr. Smith" and he says, "Kevin Szczepanski?" I say yes, he says I have your laptop. And I quickly said, and I have yours, don't I? And he laughed and we talked for a bit. Turned out he was an information security specialist at a company in Florida. We were both, you know, one behind the other in the security lane. I said, you know, I'm so sorry, I must have been distracted. I had a pretty heavy pat-down. He said, yeah, I saw that pat-down. It was pretty heavy. And I said, well, thank goodness that you're an information security specialist, and I'm a data security and technology lawyer. Because this may have a happy ending. And, you know, in the back of my mind, I was thinking, be careful, Kevin, you don't know who you're talking to. This could be a threat actor who's pretending to have your laptop. But in the course of the conversation, I realized it was all true. I had his laptop, and he had mine. And I said, you know, I'm so grateful for your call. There really was no way for me to make a similar call to you, because your laptop is off and it's out of power.

[Kevin]: He said, well, the reason I found you is that I opened up your laptop and on your lock screen is your name and your photo. So I googled your name. I satisfied myself that that was you in the photo. And using your contact information, I called your office. So from then on, we talked for a little bit. We arranged to ship each other's laptops back to the other overnight, and the long and the short of it is, it worked out. I got my laptop back. Mr. Smith got his laptop back and everyone was happy. So why am I telling this story? I mean, I don't know if you've noticed this. I have noticed it. People in the cyber security world, people in the information security world, are not particularly anxious to tell you about the mistakes that they make. Because if they do, then you start to think, well, if you're careless about your laptop, what else are you careless about? But I thought about it and decided that I would share this with you, because I think that we all have a kind of reluctance to share our bad stories. But maybe if I share my bad story with you—which turned out well, it was a happy ending—we will all realize that we're in this together, that we all suffer from the same stresses and strains. And maybe by hearing my story, it's somewhat of a learning experience for you.

[Kevin]: So what did I learn from the happy ending—lost laptop? I think the first thing I learned was slow down and pay attention. I didn't realize it at the time, but there was a way for me to know immediately that the laptop I picked up that in every respect but one was identical to mine actually had a tag on the bottom of the laptop that says property of Barclay Damon 7000. So if I had just picked up the laptop and flipped it, upside down, I would have seen that it wasn't mine and I would have been able to exchange it right in line with Mr. Smith, and we both would have went on our merry way and wouldn't have had to ship each other's laptops back. So that's number one.

[Kevin]: And, I guess the second thing I learned is it can happen to anyone, and it often happens at the most stressful, distracting times. So think about it. You would be cautious about setting your laptop down anywhere and walking away from it from a time, because we all know that there are risks: that it could be lost, it could be stolen. But here I did that at the airport while I was going through a TSA checkpoint. So what did I learn from this lost laptop incident? I'll tell you. First and foremost, I learned to slow down and pay attention to what I'm doing, especially when I'm carrying my laptop—it has all sorts of critical information on it—through a public place, like an airport. If I had been going slower and paying attention to what I was doing, that incident might not have happened. Second thing is, I didn't know or I forgot that I knew (better said) that there's a tag underneath my laptop, so if I had just flipped it over, I would have seen no property of Barclay Damon tag in sight. And I would have known that as much as it looked like my laptop was on my laptop, and I could have exchanged it with Mr. Smith on the spot, we would have gone our merry way and there would have been no incident.

[Kevin]: So those are the things that I learned. I also learned that I was lucky, right? I lost my laptop in the hands of an information security expert who had every bit the same incentive as I did to trade the laptops and get them back in the proper hands. If it had been a thief or a threat actor, I wouldn't have been as lucky and I



would have had some 'splainin' to do as, Ricky Ricardo used to say. So I learned a valuable lesson that I didn't have to pay for, but I wanted to share that with you so that, you know it happens to everybody. It happens to me. Hit me up in the comments if it's happened to you and how it worked out.

[Kevin]: But I want to close this episode by giving you a few tips on what you do when you lose or you think you've lost your laptop. So step one: contact at your IT department. Your chances are the laptop you've lost or misplaced belongs to your employer. So you know you don't have your laptop because you lost it. So tracking down someone's laptop and going on YouTube or watching videos on how you track down your lost laptop, that's not going to be as valuable to you as immediately contacting your IT department, and we'll talk in a minute about what your IT folks will do. Second thing, change all your personal passwords. I know it's inconvenient. I know that probably you won't have to, but you really should as a precaution. Because if someone has your laptop and it's not locked and they're able to gain access to it, they're going to do a search for passwords, especially if they're a threat actor. And they're going to find your passwords, your password to Netflix, your password to your bank account, your password to everything you do, everything you are, and you don't want to give that up. So step two is change your passwords.

[Kevin]: And the third step I would encourage everyone to do is, depending on the results of your IT department's investigation, you want to contact your attorney and probably not your attorney but your employer's attorney. Because if you have lost your laptop and your IT department tells you that yeah, information in your email account, for example, might have been accessed, you or your employer might owe a disclosure obligation, and your lawyer is in the best position to tell you whether you have to give notice to any affected individuals. So those are the three steps I would take right away. You can watch all those YouTube videos on how you can find your laptop in a remote place. But if you do that, my belief is that precious minutes or hours are going to be lost, and it's best to just bite the bullet and let your employer; let your IT department know right away.

[Kevin]: Now, what is your IT department going to do? Here are the steps I think every great IT department is going to take when they find out that you have lost your laptop. Step one. They're going to verify the last time it was connected to the internet and compare it to the last time the user used it. That's how they're going to figure out whether there has been any unauthorized access to your laptop, your systems or your data. Second, they're going to check the sign-in logs for your account. This is more for peace of mind than anything else, but yet another potential indication of compromise. Number three, and assuming that your employer has the software in place to do this, they're going to set your laptop to wipe, which will happen the next time it connects to the internet. So, assuming that you contact your IT department right away, they're going to set your settings to wipe. And if there is a threat actor who has access to your computer and he or she gains access to the internet as soon as he or she does so, all of your systems and data will be wiped clean so that the threat actor gets no access.

[Kevin]: Fourth, your IT department should report the service tag number of the lost laptop to Dell or whoever the manufacturer is. And the reason for this is that your service tag number goes on a list in case someone places a service call for that laptop. As soon as they do, then Dell or the manufacturer is going to know it's been stolen. Fifth, and finally, you are going to report the lost laptop to the police. File a police report. That way, if anything ever happens, a third party is victimized by a loss of protected data or commercially sensitive data, you will be able to document that you filed a police report. And although it's often very difficult for the police to take action, it's possible that the police will be able to investigate, recover that laptop, and bring the criminal to justice. So those are all the things that you should do if you actually do lose your laptop. And hopefully you found my story to be helpful.

[Kevin]: Think of all the times you came this close to losing your laptop or leaving a precious device behind, and all the risks that could pose based on all the data that you have, not only yours, but the data of your customers, clients, patients, whoever they may be. So the start of season four of Cyber Sip, I guess the main



message is: be careful, be calm, and take your time. I know I've learned that lesson, and if you have any thoughts about my story, what you should have done differently, Kevin. Or how could you do that, Kevin? Hit me up in the comments. And, we'll see you on the next episode of *Cyber Sip*. Thanks so much for joining us.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, and Spotify. 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.

