

OK at Work: Safeguarding Your Business Data

[00:00:00]

Sarah Sawyer: Welcome to this week's OK at Work with myself, Sarah Sawyer, my colleague Russell Berger, both attorneys at Offit Kurman, and today we are talking about security as it relates to, business information. Client lists, any type of private information that you might have as a company.

Whenever we talk about security as it relates to businesses, I always think of the everlasting gob stopper in Willy Wonka. I just can't help it. That is my reference whenever I think of that, the secret sauce and those types of things. But obviously a lot of businesses have very sensitive information, whether it's their own personal business information or whether it's information that is provided to them by a client or by customers and employees, and lots of people have access potentially to that information. So what are some things that companies should be thinking about when it comes to that valuable [00:01:00] information? The everlasting Gobstopper recipe, the client list, the customer data.

Russell Berger: Yeah, you should definitely not have a tour of your factory with a bunch of kids that want to get into everything. If you want to keep your trade secrets a secret. But I know Willy Wonka had other purposes for doing that. In any event, no, I mean at its core, things that are secret and confidential and proprietary should be protected that way.

It's even in the law when you look at the trade secrets law, various laws. Part of the way you determine whether something's a trade secret is do you act like it's a trade secret? Do you protect it or do you leave it laying around and do you give the secret formula to everybody that comes in the door.

So just as a starting point, the stuff that's really important and really proprietary should be, limited access, should be protected, should be secure in whatever way makes sense, given your IT infrastructure and or the tangible infrastructure that you have in your workplace.

And to take that a step further, one of the things that I think you can do as a business owner to [00:02:00] police and protect your information security is to just keep an eye on what things are being downloaded, what's being accessed.

And this isn't to go like full big brother and monitor what everyone's doing on your system.

But, there are certainly alerts that you can work with your IT teams to set up, to tell you if, certain information's being accessed or certain volumes of information are being downloaded. That's one of the things we see a lot of when employees departing from one business to go to the next is they want to take a whole bunch of stuff with them, and all of a sudden, their download levels on a daily basis are nominal. Then you get this giant massive of download all of a sudden to an external hard drive and you say, okay what's going on here? What warning signs should I be reading from this?

Or, all of a sudden there's a whole bunch of emails being sent out to a personal email address forwarding a bunch of documents. And those are things that, again, you shouldn't be personally looking over all these things, but you can set up alerts to help monitor.

And again, it's just really important to, protect that gobstopper formula.

Sarah Sawyer: Yeah, and it's good to have a sense, and I [00:03:00] think technology can really help you here to your point, Russell, setting up alerts, figuring out how you might be able to monitor for those things where stuff is stored.

Making sure that people are storing things in the proper place, not locally on their hard drives, especially if they're a remote employee. And, they've got their equipment wherever they are and just making sure that you've got all those things in place. But also another thing I see is making sure that, if you are gonna use technology to help monitor these things and keep track, know what your technology is doing.

I've had clients who have suddenly realized that, to your big brother comment and looking over people that they realize they're looking over people and they don't even know it. So you wanna make sure you know what you're doing and have those tools, working appropriately and storing the things you want them to store.

And, I try to stay up with the times as it relates to tech. I could not tell you exactly the inner workings of all of that and what that looks like, but you probably have someone on your team or someone externally that you work with that can help you with that. And it's important to just have a good sense of what's possible and how all that works for that [00:04:00] reason.

Russell Berger: Yeah, it's the question you should ask. Using a physical property as a metaphor here, do you have cameras covering the exits? Do you have, cameras on the windows? What are your weak points and what are you doing to monitor them?

And I think it's the same thing from information security and protection. And again, part of that is firewalling and putting the important stuff in the vault. And the other part of that is monitoring what people are doing to try to pull information out.

Sarah Sawyer: Yeah, well, definitely ought keep track.

But thanks Russell. We'll see you next time.

Russell Berger: Thanks Sarah.