Podcast

Technologies and the Life Sciences Industry

By Margaret J. Strange & Mary T. Costigan

June 18, 2024

Meet the Authors

Margaret J. Strange

(She/Her)
Principal
(860) 331-1554
Margaret.Strange@jacksonlewis.com

Mary T. Costigan

Principal
908-795-5135
Mary.Costigan@jacksonlewis.com

Related Services

Life Sciences

Details

June 18, 2024

As life sciences companies research, discover and accelerate their product advancements to improve lives, they strive to avoid risks to the privacy and security of their sensitive data and company systems. However, emerging technologies, remote work, and international travel among employees bring privacy risks that demand immediate attention.

Jackson Lewis P.C. · Technologies and the Life Sciences Industry

Listen on Spotify
Listen on Soundcloud
Listen on Apple Podcasts
YouTube
LISTEN ON libsyn

Transcript

Welcome to Jackson Lewis's podcast, We get work™. Focused solely on workplace issues, it is our job to help employers develop proactive strategies, strong policies, and business-oriented solutions to cultivate an engaged, stable, and inclusive workforce. Our podcast identifies issues that influence and impact the workplace and its continuing evolution and helps answer the question on every employer's mind. How will my business be impacted?

As life sciences companies research, discover and accelerate their product advancements to improve lives, they strive to avoid risks to the privacy and security of their sensitive data and company systems. However, emerging technologies, remote work and international travel among employees bring privacy risks that demand immediate attention. Failure to address these issues can inadvertently expose the company to significant litigation and regulatory risk.

On this episode of We get work™, we discuss how life sciences employers can effectively manage data privacy, cybersecurity, compliance, and risk while sharing a few examples and recommended best practices. Today's hosts are Peggy Strange and Mary Costigan, principals in Jackson Lewis' Hartford and Berkeley Heights offices. As co-leader of the Life Sciences Group, Peggy provides clients with innovative support and straightforward plain language information on emerging client issues. Mary, a member of the Privacy, Data and Cybersecurity Group, holds a Certified Privacy Professional designation from the International Association of Privacy Professionals. Mary advises multinational, national and regional companies on emerging privacy and cybersecurity issues.

Peggy and Mary, how can life sciences employers ensure good privacy practices, and how does that impact my business?

Thank you, Alitia. We are happy to be here today with Mary, who has helped me certainly see all the emerging and existing issues around our technology. We talk about technology all the time, and Mary and I recently had a conversation that was really eye-opening to me, all the things we should be doing. We're always playing catch-up with technology, and Mary has taught me some things we can do to get ahead of it in simple ways that we hadn't been focusing on. So with that … I'm going to ask Mary, you know, we hear so much about, particularly in life science, all of the travel everybody's doing, right? Our employees are traveling around the world for work, for fun, or working remotely. What should our life science clients be thinking about when their employees grab their laptops and head overseas that maybe they're not thinking about now?

Hi Peggy, it's nice to be continuing this conversation with you again. And that's a great starting question. So any mobile device that can connect to the company's electronic systems or otherwise access the company's data can present a risk to the privacy and security of those systems and data. We're talking about mobile devices. That's a laptop, a cell phone, a smartphone, maybe a tablet. So any of those devices. And we're talking about not only the company's systems, but their data, which runs from personally identifiable information to proprietary information, operational data, financial data, customer or client data. So there's a lot of data in scope here for purposes of this discussion. So when an employee travels overseas with one of those devices, particularly to what's called a country of concern, those risks to the data in this company's systems increase. So we know we have those risks on a daily basis and we work to try to minimize those.

But once they're traveling overseas, those risks increase, in some cases, exponentially. And how that increases, malware can be downloaded without the employee's knowledge if they connect to public Wi-Fi. Say at a hotel, maybe an airport, the coffee shop, a public charging station, or even if they're connecting to a printer at the last minute to get some documents printed out. The device can be hacked so they can access or use that device to attack the company systems. So they can then deploy ransomware or malware in the systems, or they can steal data from the company systems. They can corrupt data.

A lot of this can do significant harm to the company. They can access data that's already been downloaded to the individual's device. They can access contacts that are on the device. They can access the employee's emails. So all of this can lead to sensitive information being subject to unauthorized access or maybe getting information on what the company's doing overseas for business.

The things that scare me are the ones that they can activate the microphone or the camera in the device so that they can eavesdrop on sensitive conversations or maybe even record them. And they can activate the GPS so they can track where the employee is going, maybe find out what competitors are going to, or maybe just to track the employee. That's a little bit unsettling in terms of employee's safety. And also the last one, where customs may confiscate the device or they may review it before returning it to the employee. So all of this can lead to a third party

gaining access to sensitive data or the company systems. And again, this is a tremendous risk depending on the type of company in their business.

So what are ways to minimize this risk? I think one of the best ones is to draft an internal employee policy. That policy would address the permitted and prohibited practices for using these devices when going overseas. It can apply maybe to not only company-owned devices, but also personal devices.

Another aspect is training employees on the proper use of their devices, how to configure security settings, how to make sure that they're securely connected to the company's systems, how to erase data, how to delete certain apps when they're going overseas, how to update and patch any software to make sure it's secure.

Another possibility is requiring employees to submit their devices to the IT department who would inspect them to make sure the software and security features are updated and patched prior to travel or even requiring them to submit their device to IT when they return. So IT can wipe it and clean them before the individual or the employee reconnects to the company's systems.

So there's a lot to be considered here. It's going to be scalable depending on the company and where the employees are traveling and what the company does. But it's an area where legal, HR, and IT will all want to play a role in drafting those policies and developing that training.

One last option is, if the company is able to, it may want to provide the employees with a clean loaner device that can be used and returned to the U.S.

Right. So at least drafting an internal policy to get everybody started would be helpful. And on another topic, Mary, as the size of data and emails grow and we get companies that call us and say, you know what, we have so much data. Can we just delete stuff? What should we be doing about retention policies and schedules? And I'll ask, hey, can we look at your retention policies or schedules and find out they haven't looked at them in years? So what are some of the best practices for retention policies and schedules?

So I'm going to look at this from a data breach perspective. Part of my practice is I do a significant amount of data breach response. And we're seeing a large uptick in business email compromises. And that means a threat actor or a bad actor, as they're called has obtained the legitimate credentials of an employee for their email account. So that means they have the actual username and the user password. And they can access that employee's email account and move around in that email account looking at emails and folders and attachments freely because they have legitimate credentials. And they can get these credentials either through a phishing email where the employee gave the credentials unknowingly. They can buy them on the dark web if they were part of an earlier breach. Or they can just hack in.

So once that threat actor gets inside that email account, any sensitive information that employee has in there is subject unauthorized access, which down the road could potentially be a data breach. So one of the things that's been coming up with us when we talk clients through this is we realize how much, when they

realize how much information is in that email account. So it goes without saying the more information, more emails in that account, the more likelihood there's sensitive data that could be subject to either unauthorized access or theft.

So I'll give you an example. I had an HR manager recently who had an email compromise. We talked about what she has typically in that account, and she told us that she had outsourced all HR functions. So she no longer received any sensitive information or sent any sensitive information through her account. They had outsourced five years ago. So it was looking good. It looked like there was no data breach.

The next day after doing some further forensic review, we determined that the email account had 10 years' worth of data, 10 years' worth of email. So, although they outsourced payroll functions five years ago, there were still five years' worth of W9.

So having an email retention schedule that is appropriate to the nature of the employee's role and responsibilities is addressed or drafted in conjunction with legal understanding the different ramifications and laws with respect to deleting that account is important. If an employee has sensitive information that they regularly handle, perhaps in helping them or providing them tools to remove those sensitive emails immediately from the email account and storing them in a secure location. So in the event of a breach or unauthorized access, the account does not have those sensitive emails. So it's an interesting area. It's not one that is on many of our radars, but it's definitely an area worth looking at in terms of not only developing a sense of what's in your email account, addressing how long you retain that, and also including emails in your retention schedule.

Perfect. And then what would our life science clients need to be thinking about, Mary, in regard to access controls?

Yeah, that's a great question, Peggy. You and I have been talking about this a little bit. And I actually have two cases right now where we're dealing with employee access to information that they should not have had access to.

So access refers to the ability of an employee to access the company's systems or certain data. So to protect the company's systems and data, we recommend that the employee only have access to what they need for their role and responsibility, sort of a need to know. So when you give an employee unfettered access, the risks to the company's systems and data increase. So we see this come up frequently in a few scenarios where there's a disgruntled employee or employee who's planning to bring a claim against the company, for example, a discrimination claim. They may be searching through the company data or the systems to find information they can use against the company or to support their claim. We may see employees who are about to leave the company and they start to take information about the company's operations or a customer list for their new job. Oftentimes this isn't found out until after the employee is left.

Going back to the data breach, when a threat actor steals the employee's credentials to get into the system, it has as much access as that employee would have based on their access privileges. So the more access that employee has, the

greater the access the threat actor has.

And then the last one is there's always the employee that is simply curious and looking to see what's on the systems. Not as harmful, but not something you really want happening.

So action items here is, again, it's all about drafting those internal policies that require reviewing the access level for each employee based on their role and the work that they're doing and working with IT to provision it. And then periodically reviewing access levels to ensure that they are appropriate as the company grows and the organization changes. And then anytime an employee is promoted, whether they're transferred or they're terminated, making sure those access controls are adjusted appropriately or terminated. That's very helpful. We hear a lot of stories where employees access information they shouldn't have accessed and the client's responses. Well, shouldn't they be disciplined? But in reality, they had access to it. Whether you like it or not, you probably shouldn't have given them access. So that's a good suggestion to limit access.

And finally, we all know employees are using ChatGPT or something similar, whether we like it or not. Everyone's sneaking a peek to see if it could help them. There are so many concerns in this area, but specifically, what are some of the best practices related to protecting privacy in this area?

Right, so that's an interesting question. We're hearing a lot of discussion about using AI tools in the HR space for employment decisions. And there is definitely some serious risks, but there are also privacy concerns, as you noted. And a lot of them revolve around what can the tool do? What is it supposed to do? What data is the employee putting in there? What are they permitted to put in there? Are there any controls around what the employee can put in there? If they are inputting data, will that data violate the company's privacy policies, the disclosures that the company made to perhaps a data subject about their data and how it will be used or disclosed? So there are a lot of issues arising out of use of potentially personally identifiable information. If an employee inputs certain data, they may be the output. They may be creating an inference or profile that now constitutes personally identifiable information, depending on the data protection laws.

And if the company is not aware of this, it may be violating those laws and its obligations to personally identifiable information. It may not be retaining that data in accordance with its data retention schedules. So again, knowing what's being input or could potentially be input.

There may be contractual obligations the company has with third parties. For example, we're seeing more provisions in services agreement that restrict the use of AI by the vendor. There's the possibility that the tool could create a vulnerability that could be exploited for cybersecurity attack. And we're also seeing the potential for these tools to create data leakage, more often incidentally.

So using this data in a variety of ways that is still, I feel like it's the new frontier, understanding these tools, using them appropriately, auditing those tools to ensure that the settings are configured properly, that there's no data leakage,

ensuring that the employees can't override certain security configurations is important. Drafting that employee policy that is permitted uses and prohibited uses, permitted tools and prohibited tools that monitors the output, that monitors the type of data going in and out is all very important.

But maybe the most important thing is training those employees on a regular basis to understand how to use the tools, what's appropriate use, but also giving them that ability to internalize the risks. I think you could use the analogy of phishing security awareness training here. We do so much phishing security awareness training that employees have internalized that ability to recognize something or question whether it's a phishing email. I think the same could be true here, getting employees to that level where they start to question, is this a risk? What am I doing? What's the potential output and what should we be doing with that? So again, it's all about the policies and training.

Let me just give you one example before we end. So I had heard recently from somebody that they were being sued because an employee had written a document as part of their normal responsibilities. And that document contained typical customer information. But then the employee decided to run it through an AI tool to help edit and improve his writing. And that resulted in a data leak of the customer's information and then lawsuit. And when the employee was questioned as to why they did that, the response was, well, my manager told me I needed to work on my writing. It's the obvious ways we might expect risk, but also some of the unobvious ways when employees are trying to do their best.

Sure. So perhaps the manager didn't mean work on your writing by going on AI and have it rewritten, but the employee was doing what the manager said, working on their writing.

Exactly.

Well, Mary, thank you so much. My takeaway is where everybody should have a policy around international travel. When you grab that laptop and go, we should look at email retention and schedules based on the employee's job, which I had never thought of, limiting access for employees to the computers for the information they just need for their jobs, and then know what employees are doing with AI and training them to understand the appropriate and, more importantly, sometimes inappropriate uses of AI.

Thank you very much, Mary, for your time today. And I look forward to ongoing discussions around all these fascinating, and more importantly, topics that we're hearing more about from our life science clients.

Thanks, Peggy. It's always a pleasure.

Thank you for joining us on We get work™. Please tune into our next program where we will continue to tell you not only what's legal, but what is effective. We get work™ is available to stream and subscribe on Apple Podcasts, Libsyn, SoundCloud, Spotify, and YouTube. For more information on today's topic, our presenters, and other Jackson Lewis resources, visit JacksonLewis.com. As a reminder, this material is provided for informational purposes only. It is not

intended to constitute legal advice, nor does it create a client-lawyer relationship between Jackson Lewis and any recipient.