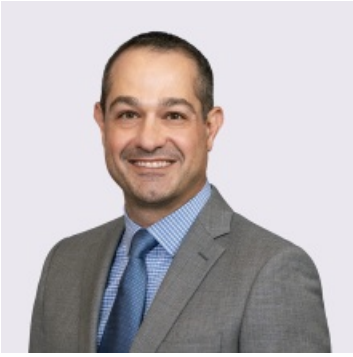
Podcast

Living and Working Outside the Firewall: Is Your WorkHouse Secure?

By Jason C. Gavejian & Joseph J. Lazzarotti

December 10, 2020

Meet the Authors



Jason C. Gavejian
Office Managing Principal
908-795-5139
Jason.Gavejian@jacksonlewis.com

Joseph J. Lazzarotti
Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Related Services

COVID-19
Privacy, Data and Cybersecurity

Details

December 10, 2020

A remote or hybrid-work environment presents privacy, confidentiality and security challenges that either were non-existent prior to March 2020, or at least not at pandemic level magnitude. Device usage, network access, data security and document retention are among the issues requiring employers to revisit protocols and user training to minimize risk.

Jackson Lewis P.C. · Living and Working Outside the Firewall: Is Your WorkHouse Secure?

Listen on Apple Podcasts
Listen on Google Podcasts
Listen on libsyn
Listen on pandora
Listen on Soundcloud
Listen on Spotify
Listen on STITCHER
YouTube

Takeaways

A remote or hybrid-work environment presents privacy, confidentiality and security challenges that either were non-existent prior to March 2020, or at least not at pandemic level magnitude. Device usage, network access, data security and document retention are among the issues requiring employers to revisit protocols and user training to minimize risk.

What Employers Need to Know

- Employers are increasingly looking to technology to address concerns about employee productivity in the remote workplace including:
  - Key logging software;
  - Network activity; and
  - Audio or network monitoring.
- Striking a balance between utilizing technology to ensure productivity and an employee's privacy or security expectations is key.
- Data security and remote working has created additional compliance issues.
  - There are a number of local, state, federal and international laws that are potentially triggered by data collection — each imposing varying obligations for employers.

    - The industry in which you operate may impose additional privacy and security regulations, i.e. healthcare, government contractors and professional services.
    - There can also be contractual provisions governing the collection, storage and destruction of data.
- Securing systems in this environment is challenging on its own.
    - Clients are looking to third party vendors to handle the enormity of the task.
    - ADA concerns are raised when new accessibility measures are enacted.
    - The use of personal devices raises issues around access, security and destruction of data.
- Employers need to allocate adequate resources now and, in the future, to help the organization meet the challenges posed by a remote workforce.
- If your company does engage in employee monitoring, ensuring those monitors are properly instructed is imperative to avoid HR issues and possible litigation.
- Training on security risks and procedures, company policies, acceptable use of devices, etc. is imperative in this new environment.
- On the technical front, encourage employees to change passwords, discourage the use of personal devices where possible, implement device management software when personal devices ae in play and look for open ports on your network.

Transcript

Alitia (00:06):

Welcome to Jackson Lewis' podcast, We get work™. Focused solely on workplace issues everywhere and under any circumstances, it is our job to help employers develop proactive strategies, strong policies, and business oriented solutions to cultivate a workforce that is engaged, stable, and diverse. Our podcast identifies the issues dominating the workplace and it's continuing evolution and helps answer the question on every employer's mind. How will my business be impacted? A remote or hybrid work environment presents privacy, confidentiality and security challenges that either were non-existent prior to March 2020, or at least not at pandemic level magnitude. Device usage, network access, data security and document retention are among the issues requiring employers to revisit protocols and user training to minimize risk. This episode of We get work™ offers best practices and recommendations that employers can follow to ensure the highest levels of privacy and security compliance are met and your business is protected.

Our hosts today are Joe Lazzarotti and Jason Gavejian both certified information privacy professionals by the International Association of Privacy Professionals. Jason and Joe are leading by example, working safely and securely from home in New Jersey to help clients meet privacy and security challenges, challenges that appear to multiply at a rate that is almost as fast as the increasing number of days of the pandemic. Joe and Jason, the question on everyone's mind today is what can I do to ensure compliance with privacy and security regulations and protocols? And if I don't, how will my business be impacted?

Joe Lazzarotti (02:00):

My name is Joe Lazzarotti. I co-chair our Privacy, Data and Cybersecurity practice group. I'm here with my new co-chair Jason Gavejian. What follows is not unlike conversations Jason and I have had in each other's offices trying to work through complex data privacy and security issues for clients, except we're not in the office, just as millions are trying to adapt to a remote work environment, businesses and organizations have had to adapt as well. At the [inaudible 00:02:33], many face this transition with lots of questions about how it might affect their businesses and some of those questions remain. Many of those questions raise significant privacy and security issues. So we thought we'd post some of those questions that we've received and talk about them. Maybe a good place to start J, is productivity. Businesses have been concerned about how are we going to keep employees productive during this time? Different types of technology, different types of industry, different needs of businesses management styles. So how do we use technology? What have we seen on that side?

Jason Gavejian (03:10):

Yeah. So that's an issue that I think most employers are currently struggling with or are certainly concerned about. Interestingly, I didn't get as many questions about employee productivity pre pandemic, so I'm not sure if employers think that's simply because their employees are now remote, that they can't rely on them to complete their work. The hope would be that all of us are adults and can be responsible for the work that we have to do on any given day. But unfortunately in reality, that doesn't always work out that way. So as you know Joe, we've had some pretty interesting client conversations about potential monitoring of their employees in ways to ensure productivity, whether it be implementing something like key logging software, where you're tracking everybody's keystrokes throughout the day, whether it be tracking network activity to see when somebody might be logging in or how active they are throughout the day. That's probably the best one, especially if someone's logging in through your company's electronic systems.

But we've also had some rather interesting inquiries related to either audio or even video monitoring. Not one of the most interesting ones that I'm thinking about is we had a client who was proposing to utilize in-home webcams to 24 hours a day, seven days a week, monitor employees the way they explained it to us was similar to looking through someone's home security cameras, couldn't we just set something up like that to ensure that the employees are actually at their desk or at their computer throughout the Workday? As you can imagine, we advise strongly against that. There's a number of issues with the amount of data that might be collected, the information that you might glean about an employee, or certainly risks that you'd capture information or images that you otherwise wouldn't want as an employer.

So trying to find that balance between utilizing technology to ensure productivity and then considering what the employee's privacy or security expectations might be is really a key. There's also a number of other issues that come into play when we're talking about monitoring, whether it's being in a state like California or the

CCPA, the California Consumer Privacy Act would require notification to any employees who we are going to be monitoring or collecting personal information about, whether it be a state like Connecticut or even Delaware that have electronic notice requirements with respect to electronic monitoring, or if we're capturing large amounts of data about employees, we might have ADA concerns, GINA concerns, or state medical privacy concerns. And certainly if we are implementing at home monitoring or video monitoring, we may gather that type of evidence or that type of data, even if we don't want to. This doesn't mention concerns under the GDPR or cross border data transfer issues, which frankly could be a podcast in and of themselves.

Joe Lazzarotti (06:00):

Yeah. I recall doing a podcast, not a podcast, a webinar, and it was being recorded. And I thought I was doing a real good job until I saw somebody in the lower left-hand corner, pretty much laying down and asleep on their desk. So either I wasn't doing a good job or that recording wouldn't be a good sign of productivity for that organization. So I [crosstalk 00:06:21]. That's right, that's right. Interestingly, along the lines, I got an email today about a client looking to monitor the screen time of employees. I quickly thought about my 16 year old and my 15 year old who we monitor screen time a lot. So there is certainly a lot of this going on, but I guess one question also that businesses are asking is thinking about, "All right. Yeah, this all sounds great, but what are the compliance requirements?" I mean, can we even do this in terms of monitoring and getting involved with looking into people's homes, using their devices? What are some of the issues there?

Jason Gavejian (06:58):

Yeah. So again, I think that there's a lot of high level concerns that we'd want to be conscious of whether they be industry considerations. If you're in the finance industry, healthcare providers certainly governed by HIPAA and had additional or heightened security requirements if you're a government subcontractor or even a professional service provider, like a lawyer, CPA, et cetera. You may have additional considerations as to what you need to safeguard again, based on an industry standard, not to mention some of the legal requirements. I know that you deal with a lot of those pretty regularly, Joe.

Joe Lazzarotti (07:32):

Yeah. I mean, one of the things that clients have thought about in the last few years is maintaining data security, right? We've come across clients that are in Massachusetts and be dealing with the data security regulations there, as well as you mentioned the CCPA earlier. And that itself has some data security provisions in that, it has a private right of action. There's a data breach, the New York Shield law or the law in Colorado. So there's been a bunch of laws that deal with maintaining data securely, as well as some of the privacy issues that you raised earlier in taking reasonable steps. I mean, that's pretty much the standard. There certainly are a lot of specifics, but there are reasonable standards, reasonable steps that companies need to take to maintain security. At the same time, there's obligations to the extent you're using certain platforms, certain vendors, if you as a business or an organization are a vendor, you may have contractual obligations

that you're subject to in order to make sure information is maintained and transmitted securely, including with regard to employees that are working remotely.

I've seen certainly some contractual provisions that require the company not to allow data to go outside of its environment, which means if you haven't carefully gone through your work from home policies and procedures and employees are using personal devices that could be an issue. Also, we see this also not just with personal data, a lot of times the focus is on personal data, but businesses that are in construction, businesses that do government contract work and others, they're oftentimes dealing with a lot of sensitive intellectual property trade secret information and other data that can be compromised, lost, or shared outside of contractual provisions in the process of working from home. So certainly thinking about compliance is critical and also thinking about even if we're allowed to do it, are we contractually bound ourselves to not do it? And for organizations that have any professional responsibilities, I know we do as lawyers, there's also rules of professional responsibility that requires to think carefully about these issues and take appropriate steps to safeguard any data that we're handling.

Jason Gavejian (09:56):

Yeah. I think that for me, most of the questions that I get, whether from clients or colleagues relate to what are the laws or the regulations that might apply here. Oftentimes, those clients or colleagues are overlooking that, as you said, there may be contractual requirements, which not only from a business standpoint, but also from a legal standpoint are something that should be considered. I really think that all of this comes down to the main question of whether or not this switch to remote work means that we're really less secure. And if so, why? Well, I'm glad that we're on a podcast today as opposed to a video conference, because I don't look as tired when I'm on a podcast so [inaudible 00:10:36] can see me.

As employees are extremely tired, they're stressed, they're overwhelmed. They're trying to navigate having their children at home. They're trying to navigate their concerns about COVID and what impact that may have on their life. They're typically going to be paying less attention to what they would be doing at work. And certainly as we all move to this remote work environment, and many of our daily transactions or daily communications are conducted via email or over the internet, there's going to be an increased risk of someone simply clicking on an attachment or opening an email just because they felt as though this was a quick way to get something off their checklist on any particular day.

What this leads to is potential ransomware attacks, where someone clicks on a email that they believe to be legitimate. And now they've downloaded software onto their system, which encrypts all of their data and causes them to have to pay large amounts of money to threat actors in order to free up their data. Or it potentially leads to business email compromise matters where it's just because someone clicks on a link or provides access to their email account now the threat actor has potential access to all of the information in that account. Again, when we're dealing with employees who are new to a remote work environment and already under a lot of strain the chance or the increased risk here is significant.

This doesn't mean-

Joe Lazzarotti (11:59):

J, you've seen those increases, right? You've seen the attacks on companies, right? We've seen that.

Jason Gavejian (12:05):

Oh, absolutely. I think that we obviously work with a number of carriers and a number of internal clients on data breach response or data incident response and we've seen a significant uptick. Unfortunately, these threat actors are the bad guys. So they do their best to take advantage of situations that all of us are struggling to deal with. And certainly COVID-19 is one of those. Now we've seen a lot of the business email compromise, or even the ransomware attacks referenced COVID-19 guidance, COVID-19 business protocols, things that employees would be expected to look at and to understand, and again, the threat actors are utilizing those to perpetrate their attacks. One of the other big considerations for me is on the IT front. When back in March, everybody jumped to remote work we really did so virtually overnight and many clients or many businesses were frankly not prepared for that.

And if the systems were not able to handle that bandwidth, it could strain the network and certainly could create additional security risks about whether or not the network is unsecure or whether or not it's actually able to support the requirements for security based on the number of people who are entering the system at any given time. This also doesn't account for employees who are connecting to unsecure connections, whether it be at their local coffee shop, or as I think the statute of limitations on this is probably run at this point. But I got to think I'm not the only one who at some point borrowed a neighbor's wifi, whether I was living in an apartment or a condo at the time in order to make sure that I was able to get onto the internet.

In those situations, that network may not be secure. It may be subject to a different security requirement and certainly could expose your organization to some risk. Additionally, and as we talked about earlier with monitoring employees, if we're tracking the employees when they're outside of the workplace, there's an additional privacy considerations that might come into play as we try and balance improving productivity, ensuring employees are doing what they should be throughout the day with an individual employee's privacy rights.

Joe Lazzarotti (14:14):

Yeah. It's funny, you mentioned IT departments. I know that's come up quite a bit, not just in the remote work, but just generally. It kind of says something about some of the challenges that organizations are facing. I know when your experience may be the same when we run up against data breach situations and you need to get data security expertise internally, sometimes the IT folks have fantastic abilities in terms of systems in basically getting the computers to come on in the morning, keeping things going, but they may not just have the kind of cyber experience that's needed to secure information. Sometimes the question to the

client is, how do you feel about your team? Are they able to do this work? Can you evaluate them? In the HR space, a part of the job is to evaluate employees and their performance. Can you evaluate your IT team? Do you know if they have really gotten your systems for remote work and as secure as they can in a reasonable way. And sometimes looking outside to third party providers is one solution to help with that.

Jason Gavejian (15:20):

Joe, just on that point, it's interesting you referenced that because I think a lot of the IT departments or what companies may consider is that their IT department may ultimately be responsible for the incident. They may miss the patch, or they may have been delayed in rolling out some updates to the system that caused the incident. So they might have a vested interest in essentially trying to cover their tracks or cover what they may have missed. And it's not always the case, but it's certainly something that, as you mentioned, a client should consider when evaluating where there IT department is in the incident response process.

Joe Lazzarotti (15:52):

Exactly, exactly. Right. And I guess not to make it sound bleak. I certainly think it's a lot of providers, some clients look to third parties to help support those efforts and I think even there, it's important to have a good level of scrutiny over the folks that you're relying on to maintain your systems, to look at privacy, look at security, not quite a remote workforce issue, but one thing that kind of raised this concern poignantly for me was we were dealing with a couple of clients that were installing kiosks for COVID screening. We were looking at the specs and saw that it said a siren will sound when the temperature is exceeded. So if you had a temperature above 100.4, and that's how it was configured to indicate someone had COVID symptoms, the kiosk would sound the siren, which for us was like, "Wow, won't that raise a confidentiality issue for all the people around them who hear it and see, now this employee has a high temperature."

We talked through some of the ADA issues with that client because not really understanding well how that technology would work, but when you walk through it, you see some issues that can be raised. So I guess that's a good segue. We've been talking about remote work, but not everybody is working remotely all the time and hopefully as the vaccine begins to come out, things will get better. People are going to start coming back and have already started coming back to the workplace and so there's even this period of back and forth. What are some of the things companies are asking that we need to think about when employees start to come back, how do we manage the devices? How do we deal with the data that may have been stored at home? So you're getting some of that J?

Jason Gavejian (17:32):

Yeah. And to your point Joe, it's not only that the business may want their employees back in the work site, but if they're anything like my wife who has to share an office space with me now, she's very excited for the possibility of going back to work and not having to share an office space anymore. So again, there may be instances where employees are pushing to go back to the workplace, or

certainly as hopefully the vaccines come about and we get COVID-19 under control that we're going to be looking to return employees to the workplace. For me, the biggest issue there is going to be personal devices and the type of information that might've been maintained on that device, whether it's information about other employees, information about customers or clients, or as you mentioned earlier, confidential or secure business information. Information that the company doesn't want out there and wants to keep in their control.

If it's on an employee's personal device and it's not subject to mobile device management software or some other security protocols that would allow the company to control that data, it's potentially going to be at risk. And in order to try and get that data back from employees, whether it be an employee who is coming back to work or an employee who decides to move on whether voluntarily or through a separation or termination, oftentimes trying to get that data to be returned in any sort of reasonable fashion is very, very difficult. So that also doesn't touch on the idea of destroying data. I'm sure none of us have a large industrial shredder at home. So more often than not an employee might be printing out data that should be stored confidentially and certainly not just thrown in the trash, but because they have large volumes of paper and nowhere else to put them, they simply throw them in the garbage and now they're frankly, subject to anybody who might review that document as part of a trash bin or looking through a trash bin to see what might be in there.

Joe Lazzarotti (19:27):

No, exactly. It's interesting when you said that employees start printing out data. Some employers will have to think about where's the line and how can they require employees. Sometimes they need to get that data back. You have some employees who print everything and there's a saying possession is nine tenths of the law, so it can become problematic to get that data back. And the question is, how far do you go? So that's a good idea at that point to really think about getting some advice on, if that becomes an issue, what steps you need to take. Then if you're dealing with certain specific information, you may have an obligation to take some steps and kind of along those lines, we've raised a lot of issues and there's certainly a lot of steps that businesses can take, organizations can take both that are much more extensive, much more time consuming and maybe more expensive in the long run, but there's also some low hanging fruit.

So what we'll talk about is in terms of next steps and roadmap to follow is not exhaustive, but it'll help you and think about some low hanging fruit and things you can do. From my perspective as business leaders, I think they have to think about giving their folks adequate resources. One of the complaints we hear a lot about from CISOs, chief information security officers, chief information officers, is that they'd love to do all these great things, but they don't have the resources. And there's a push and pull on that for sure. But it's something that [inaudible 00:20:54] has to think about particularly as this 2020 kind of winds down, it was a test. And I think a lot of businesses are really thinking, and re-imagining the workplace and what that's going to look like going forward, will it involve a greater degree of remote or flexible work?

And if so, what systems do we have to put in place? What do we need to do to make that work for us, given the experience that we had? So certainly resources will be needed for that. Another thing is if you're going to have people doing monitoring, it's important to set up a system where you're monitoring the monitors. Sometimes people who engage in monitoring can maybe go a little bit too far and they need some guidance as to how far they should go. For example, if an individual is monitoring an employee, who's on a video chat or on a WebEx. And in the background, there is information about a person's religion because of symbols that are on the wall or a child who has a disability and a medical condition that raises issues because that information could be considered in the latter case genetic information.

So what does that monitor do with that data? Do they go onto Facebook and look to find out more information about what they see inside the employee's home? Those things have to be managed and so monitoring the monitors can help. And of course, a big thing that we're seeing a lot of is training of employees and awareness. Jason talked a lot about phishing attacks, ransomware. Most of it happens through things that employees do, clicking on the wrong links, spotting emails that are fictitious, those sorts of things. Anything else J, that you think of in terms of a roadmap for employers?

Jason Gavejian (22:36):

I think for me, where to get started is really conducting a risk assessment. Especially as we've now changed systems or certainly changed electronic networks and how information is going to be flowing throughout the organization or where it might be stored. I think assessing what your data security practices currently are and what type of data might be maintained by your employees and where it might be maintained is really going to be key as you look to implement some additional steps. And Joe, I know you were talking about some low-hanging fruit earlier. What did you have in mind there with respect to what employers or organizations can do from a technical side?

Joe Lazzarotti (23:15):

Well, I think training is one thing, making sure they are good passwords. If you can avoid using personal equipment, you can certainly do that. Some companies are rolling out mobile device management. That may be a little medium hanging fruit, right? A little bit more than low hanging fruit, but it's a good step if you're going to use personal devices to protect information. You can look for ports on the system that are open. That's a popular way in for bad guys, for remote desktop protocol attacks. So those are some things that you can do pretty quickly that come to my mind.

Jason Gavejian (23:51):

Yeah. I think at the end of the day, what it all comes down to is realizing that the pre COVID world is not something that we're likely to see again, and as organizations and businesses, and certainly employers, we need to understand that and to make sure that we're taking steps to address how best to protect the organization and those who work for us.

Joe Lazzarotti (24:13):

I would say organizations really need to think carefully about the steps that they want to take to address their business concerns as employees and other workforce members perform their tasks remotely. This is not something new, but it's something more extensive and there's a lot to think about.

Alitia (24:34):

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, Google podcasts, Pandora, 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.