Lowenstein Sandler's Executive Compensation and Employee Benefits Podcast: Just Compensation

Episode 61

By Jessica I. Stewart, Taryn E. Cannataro, Amy S. Mushahwar

JULY 2026

Megan Monson: Welcome to the Lowenstein Sandler podcast series. Before we begin, please take a moment to subscribe to our podcast series at lowenstein.com/podcast or find us on Amazon Music, Apple Podcasts, Audible, iHeartRadio, Spotify, SoundCloud, or YouTube. Now, let's take a listen.

Jessica Stewart: Welcome to the latest episode of Just Compensation. My name is Jessica Stewart and I'm an associate in Lowenstein's Executive Compensation Employment & Benefits Group. I'm joined today by Taryn and Amy who I'll turn it over to introduce themselves.

Taryn Cannataro: Hi, I'm Taryn Cannataro, counsel in the firm's Executive Compensation Employment and Employee Benefits Group.

Amy Mushahwar: Hi, my name's Amy Mushahwar. I'm the chair of our Privacy, Data Security, Risk Management, & Safety Practice. So excited to be here today.

Jessica Stewart: Today's episode tackles a topic that every employer should understand where data privacy, employee benefits, and executive compensation overlap. Insider threats and how to properly conduct an investigation but based in a threat from within. We are going to discuss what insider threats are, specific risks that intersect with employment, employee benefits, and executive compensation, what triggers a cyber investigation, how to properly conduct one, and what practical steps employers can take to avoid another one. As always, this is not intended to be an exhaustive discussion and we encourage you to consult with your legal counsel and cybersecurity professionals with specific questions. To set the stage, what is an insider threat?

Amy Mushahwar: Well, that's a great question, Jessica. An insider threat in practical terms is a threat that comes from an employee, an executive, a contractor, or any person who has authorized access, or knowledge of an organization's resources, and it uses that to access whether it's intentionally, or sometimes unintentionally, to cause harm to an organization. Not all insider threats look the same. Some insider threats are malicious and deliberately meant to harm the organization, while others are purely negligent. Negligent insiders are actually the most common category of an insider threat. These types of threats can include clicking phishing links, reusing weak passwords, emailing sensitive files to personal accounts for convenience. And also, we want to emphasize reuse of

passwords. If you have an iPhone and a password keeper on your device, you should be able to see compromised passwords as you page down proof. So, very important not to reuse passwords. But traditional security tools often assume threats come from the outside. However, insider threats come from all people with legitimate access, which makes them uniquely difficult to detect and potentially more damaging. And with the rise of remote work and expanded system access, it is a problem that we are seeing more frequently as a firm, and I am seeing more frequently in my daily practice.

Jessica Stewart: Taryn, how do insider threats overlap with executive compensation employee benefits issues?

Taryn Cannataro: Anyone with access to the company's compensation, employee benefits, and/or HR files has access to a great deal of private and very sensitive information. For example, employee benefit plans such as retirement plans, and health and welfare plans, hold enormous amounts of sensitive personal information. This could include social security numbers, financial data, and protected health information. Plans that are subject to ERISA can result in a breach of fiduciary duty. A breach can expose benefit plan fiduciaries to the risk that they fail to safeguard plan assets if plan data is mishandled or if they fail to monitor third parties with access to plan data. A breach of personal health information could also result in potential investigations by the Department of Health and Human Services and/or state's attorney general and could suggest HIPAA non-compliance as well. Anyone with access to payroll and human resource files can also give unauthorized parties access to private employee information as well. This could include C-suite salaries, pending equity awards, future corporate transactions, severance arrangements… Releasing this information can be damaging both publicly and internally. Human resource files may contain personnel files, employee addresses, summaries of disciplinary actions and investigations, and even tax records. The organization can be exposed to identity theft claims and employee litigation if some of this information were to be leaked.

Jessica Stewart: Amy, what triggers an insider threat investigation?

Amy Mushahwar: Common triggers suggest the need for investigation can include the types of items like an employee requesting access to data or systems outside their normal role without a clear business need. Also, police have measures to detect that. Unusual financial activity, particularly for employees with access to material non-public information, also have means to detect all of these. Excessive or suspicious downloads. For example, an employee suddenly downloading gigabytes of data that they have never accessed before. Email forwarding to personal accounts. On an excessive basis we understand that employees from time to time might need to forward something to print, but this is monitoring excessive amounts above baseline. Login irregularities such as failed authentication spikes or logins from geographic locations that do not match that person's normal pattern, and then suspicious digital activity from an employee who's leaving the company. Especially, employees that leave the

company need to be monitored. And whether or not it's voluntary or involuntary, we find the vast majority of our insider threats that we investigate happen because someone is changing jobs and into another competitive position.

It is important to know the legal distinction between monitoring and investigating. Monitoring is ongoing systematic observation of user activity and system behavior. This is your baseline. This is typically covered by your policies and procedures and your user guides. An investigation, however, is triggered when monitoring reveals anomalies or indicators that cross a threshold warranting deeper activity. The key is to have a clear documented investigation criteria and to apply them consistently. You want to balance thoroughness with privacy. And very, very key, as lawyers are saying, have this documented. If it's not documented, you do not have a baseline in order to measure whether or not your behavior was at least commensurate with the spirit of the investigation or the experience of past process. So, as many lawyers will tell you, if it's not documented, it doesn't exist. We want to make sure the documentation's there.

Taryn Cannataro: You'll also have to balance workplace privacy expectations and any applicable state law considerations. Privacy expectations at work are limited, but they're not non-existent. So as Amy said, the company policy should make it clear that all systems are owned by the company. They should provide notice that the company has the right to monitor email, messaging platforms and file transfers and you should apply that policy consistently and avoid targeting a single employee or employees based on protected characteristics. Certain states may also require notice or consent for monitoring and recording or have their own employee monitoring and notice statutes, so it's important to be mindful of those as well.

Amy Mushahwar: I would love to add just one item that make sure you also have a mobile device management policy because any of your data crossing a telephone, you have a right to inspect and you have a right to inspect on the phone and within the primary, for example, email server, in the event that it is email. But you may need to preserve the entire device. You might not be able to legally preserve the entire device, depending on the state in which you find yourself, but reserve the right to within the policies, and that at least preserves the argument in the event that you need it.

Jessica Stewart: So once an investigation is triggered, how should an employer properly conduct an insider threat investigation?

Amy Mushahwar: Sure. Well, the very first steps are to preserve any evidence and loop in the appropriate parties. Next, you identify who should be involved in the investigation and in what capacity. Legal versus HR versus IT. Your policies typically will describe what you do for varying different pieces of investigation, and define the scope of the investigation, what systems were accessed, what data was misappropriated, whether or not the threat is ongoing and if the insider is an executive, consider whether board

involvement is warranted or required. You might need, for example, as well, forensic professionals to help you better understand the scope of the incident. Know that all of this is not decided at once, and it is typically decided in waves.

Containment options can range from increased monitoring to immediate access revocation, and the right choice depends on the threat severity and the evidence strength. Document everything to defend the company's decisions and conclusions. For example, what document triggered the investigation, what was found, what actions were taken and when. You may need this for future legal proceedings. For example, if wrongful termination is alleged, regulatory inquiries, and to improve future detection of later events. The right technical resources make or break these types of investigations. Our team has 20 plus year relationships with forensics responders. So, if you especially find yourself in a technically difficult conversation, very important to retain a forensic expert, have them retained under privilege and have them be a part of your investigation team. So, you're fully and fairly looking at this through a lens of a third party. A third party also gives you the ability for the company to have a little bit of distance between the immediate investigative function and preservation, and the ultimate investigation and legal consequences.

Jessica Stewart: After the investigation concluded, what are the key post-investigation actions and the mediation?

Taryn Cannataro: The answer here turns on whether the activity was malicious, negligent, or accidental. For example, if the breach was malicious, you may want to consider whether criminal or civil action could be appropriate. But depending on the type of breach, you'll need to consider whether the employee should be terminated, suspended, or reprimanded in any way. This is where some of the termination considerations that we've discussed in a prior episode become directly relevant. You'll need to think about the timing of the termination, if that's the route you want to take, what documentation is needed, whether you're going to ask the person for a release, and whether or not you need to pay any severance or consideration in order to get that. If the breach was malicious, it would almost certainly rise to the level of a termination for cause. A for-cause termination often triggers forfeiture provisions related to vested and unvested equity awards, bonuses, or even clawbacks of previously granted compensation. These can all be key enforcement tools in these situations.

You'll also need to consider whether disclosure to regulators or affected individuals is required. For example, disclosure may be required for ERISA plans if the breach triggers any DOL notification procedures and/or any participant communication requirements. Regardless of what type of insider threat you're dealing with, it's important to review and tighten access controls across the organization, update your policies and training, provide employees with the proper training and allow your IT, HR, legal and benefits functions on how to handle these types of threats.

Amy Mushahwar: I just want to add one tiny component to this, especially as you're investigating an IT incident, not every IT incident is a fireable event. You have to have some discretion. For example, if anyone who clicks on a malicious phishing link is terminated, that might discourage your employees from coming forward in the event that they click on a link. The same thing goes for lost laptops. So as you think of especially those negligent events, you are also weighing in that decision of to terminate or non to terminate, will something have a deterrent effect or might it actually deter good conduct which we want to encourage, which is if you make a mistake, come to IT early and we'll be able to contain the issue, contain the problem, protect consumers and protect employees.

Jessica Stewart: What are some key takeaways employers should keep in mind with respect to insider threats?

Amy Mushahwar: Insider threats are not just IT issues. They affect employment, benefits, data privacy, and could open you up to a host of legal issues, fiduciary risk, and regulatory disclosure obligations. Please, to those on the line, do not just hire a technical expert and not have that technical expert underprivileged. Do not just have IT investigate and not have that investigation being done at least under internal counsel in-house counsel privilege. Make sure that that is orchestrated if you are investigating. The key here is to plan ahead, and prevention starts with company policies and security awareness. Please have an incident response plan that contemplates insider threats. If you do not, we have incident response plans that workflow this for you. We also want you to conduct regular trainings and tabletop exercises, risk assessments and phishing simulations, and to, of course, know where your sensitive data lives and who has access to it, and have the behavioral monitoring over that sensitive crown jewel data so you can distinguish baseline user behavior between excessive behavior that might indicate a potential insider threat.

Understand what specific IT controls you have in place. As we are thinking about negligent insiders, multifactor authentication is still one of the best ways to prevent just immediate account access. We know it's not foolproof. We know MFA can be spoofed, but it should be enabled for all systems, and those that hold sensitive benefits and compensation data. One thing that I want to emphasize, and the reason why we're saying insider threats and MFA; if threat actor takes control over your user account, you typically in the immediate access, you might not be able to distinguish threat actor behavior from baseline user behavior. So, do indeed make sure that you protect against your accounts by having strong multifactor authentication. And then, compensation structure such as forfeiture and clawback can be an easy enforcement tool for dealing with insider threats. That can be a means for you to get the information that you need to get in order to secure your employees and to secure your customers.

Jessica Stewart: Insider threats represent one of the most significant and often overlooked risks at companies. Employers should ensure they have a comprehensive insider threat framework in place, maintain strong access controls and

monitoring programs, and develop trusted relationships with technical and legal resources they will need when an incident occurs. Thanks for joining us today. If you enjoyed today's discussion, please subscribe, leave us a review and share this episode with your colleagues. We look forward to having you back on the next episode of “Just Compensation.”

Megan Monson: Thank you for listening to today's episode. Please subscribe to our podcast series at lowenstein.com/podcast or find us on Amazon Music, Apple Podcasts, Audible, iHeartRadio, Spotify, SoundCloud, or YouTube. Lowenstein Sandler podcast series is presented by Lowenstein Sandler and cannot be copied or rebroadcast without consent. The information provided is intended for a general audience and is not legal advice or a substitute for the advice of counsel. Prior results do not guarantee a similar outcome. Content reflects the personal views and opinions of the participants. No attorney-client relationship is being created by this podcast, and all rights are reserved.