Cybersecurity Issues for JATCs in the Digital Age

by | **Jason Kotlyarov**

Cybersecurity and privacy threats are becoming increasingly common and sophisticated. With the advent of online instruction, joint apprenticeship and training committees (JATCs) may face increased risks.

Many joint apprenticeship and training committees (JATCs) were caught off guard last spring when they had to rapidly shift from in-person instruction to online classes.

Like most organizations, JATCs were already at risk for a cyberattack, but the hasty shift to online instruction and remote learning has increased these risks. In addition, hackers are becoming increasingly sophisticated, and their data breach attempts have become more frequent.[1]

Through efforts that include due diligence and training, JATCs can reduce the risk of a cyberattack or minimize the impact if one occurs. This article will discuss common cyberthreats and the risks posed to JATCs. It will also provide steps to mitigate these risks, and it will explore the related fiduciary obligations that JATCs may hold.

JATCs and Cybersecurity

An apprenticeship fund, or JATC, is an Employee Retirement Income Security Act (ERISA) fund that must comply with applicable employee benefit regulations. JATCs are subject to a body of regulations under the purview of the Department of Labor (DOL), the Equal Employment Opportunity Commission (EEOC), Occupational Health and Safety Administration (OSHA), and other state and federal regulations. The balancing act of running a JATC requires tremendous care, and compliance with state and federal regulations and requirements could come into serious jeopardy if the JATC suddenly becomes a victim of a cybersecurity attack.

benefits
MAGAZINE

This is because such an attack may render the JATC unable to operate or push it to the brink of financial ruin.

JATCs generally can be more vulnerable to cybersecurity threats than other ERISA plans because they often do not have dedicated staff to manage their information technology (IT), and other JATC staff members who have access to data lack an IT background.

This lack of education and failure to create sound cyber-related policies can lead to bad practices. Staff might write passwords on sticky notes left in full view, or they may fail to have effective password management policies or fail to carefully review emails from external sources. The JATC may not have email encryption or backup procedures in place or policies for securely storing and managing devices that hold sensitive data.

Moreover, JATCs and their apprentices are likely more vulnerable than ever to cyberthreats due to the increased use of online learning tools during the COVID-19 pandemic. They may trust communications that appear to come from reputable online learning providers and related parties. In addition, the use of online instruction vendors increases the number of outside entities that have access to JATC data, including the email addresses of apprentices. If those entities get hacked, it may expose the JATC to increased risks.

The use of videoconferencing platforms is another area for potential risk, especially if videoconference rooms are not password protected and file transferring features are not disabled. In addition, JATC employees may be working from home computers that are less secure.

takeaways

- The rapid shift to online instruction and remote learning has increased cybersecurity risks for joint apprenticeship and training committees (JATCs).
- JATCs generally can be more vulnerable to cybersecurity threats than other Employee Retirement Income Security Act (ERISA) plans because they often do not have dedicated staff to manage information technology.
- Although case law does not yet address liability for cybersecurity negligence for ERISA plans, the argument can be made that JATC data is an asset under ERISA and must be guarded.
- To mitigate cybersecurity and privacy risks, JATCs should conduct cybersecurity training, consider obtaining a cyberliability insurance policy and evaluate vendors.

The use of online instruction may become even more common since DOL recently issued guidance supporting the use of electronic media, including online instruction, by JATCs.[2] The DOL regulations stipulate that instruction in technical subjects related to both on-the-job learning and other learning may be accomplished through electronic media, which includes online instruction, so long as the JATC electronically transmits a written statement to the DOL Office of Apprenticeship (OA) notifying the OA that the new instruction delivery method is not inconsistent with either the JATC's current standards or its work process schedule.

Common Cybersecurity and Privacy Threats

The following is a look at common cyberthreats faced by JATCs and other organizations.

Spoofing

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source.[3] It can apply to emails, phone calls and websites, or it can be more technical, such as a computer spoofing an IP address, an address resolution protocol (ARP) or a domain name system (DNS) server.[4] Spoofing is one of the most common ways for an attacker to gain access to a system to execute an attack.[5] If a hacker were to gain access to a list of apprentices and JATC staff, the hacker could target them by sending emails that appear to be from an online course provider.

Phishing

Phishing is a method of trying to gather personal information using deceptive emails and websites.[6] The attackers masquerade as trusted entities of some kind, making it one of the oldest and most widespread cyberattack methods to date.[7] In 2019, nearly one-third of all breaches and approximately 78% of cyberespionage attacks involved phishing.[8]

Social Engineering Fraud/Cyberdeception

Social engineering fraud, also known as *cyberdeception*, is a confidence scheme that intentionally misleads an employee into sending money or diverting a payment based on fraudulent information that is provided to the employee in a written or verbal communication, such as an email, a text message or even a phone call.[9] More than one-third (35%) of large businesses and 43% of small businesses are affected by social engineering fraud attacks, and many companies are targeted multiple times.[10] Hackers and bad actors can pose as a new online learning vendor that JATC staff and apprentices are not familiar with in order to extract data about JATC apprentices and employees or to gain access to a JATC bank account or credit card information.

Ransomware

Ransomware is a form of malware (malicious software, such as viruses) that encrypts a victim's files. The attacker will demand a ransom from the victim in order to restore access to the data upon payment.[11] Typically, the encryptions in the ransomware attack are so strong that they cannot be decrypted without a key.[12] If a JATC does not have strong backup software and procedures in place, it will be forced to either pay the ransom or lose all of the data affected.

Funds Transfer Fraud

If the hacker or someone the hacker sold the JATC's information to successfully sent instructions for monies to be sent from the JATC's account to some other account, the payment constitutes *funds transfer fraud*, which is the unlawful taking of monies from an account with a financial institution because of fraudulent instruction to the financial institution to debit the victim's account and pay the money to a third party.[13]

Legal Concerns

There are several legal considerations for JATCs preparing for potential cybersecurity threats. First and foremost, JATCs are considered "employee welfare benefit plans" under section 3(1) of Title I of ERISA. Therefore, plan fiduciaries are subject to and must abide by the general fiduciary standards in Part 4 of ERISA.[14] Subject to certain exceptions, the assets of an employee benefit plan must be held in trust by one or more trustees.[15] Further, the trustees and other plan fiduciaries must discharge their duties solely in the interests of plan participants and beneficiaries for the exclusive purpose of providing apprenticeship or training benefits to participants and defraying reasonable expenses of administering the plan.[16] These duties must be performed with the care, skill and diligence under the circumstance then prevailing that a prudent person acting in a capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims.[17]

The courts are already beginning to address whether fiduciaries are liable under ERISA for failing to implement appropriate cybersecurity measures.[18] Although case law has yet to address liability in relation to cybersecurity negligence of JATCs at the time of this writing, an argument can be made that JATC data is considered an asset of the JATC under ERISA and must be guarded.

In order to minimize future risk, a JATC must use the prudent person standard to identify the best cyberliability prevention practices available and to implement policies and procedures in order to adhere to those best practices as much as possible. It is likely that in the future, either through regulation or through case law, fiduciary standards will be developed specifically to address data privacy and data integrity of ERISA funds. Until those standards are put in place, JATCs should implement the best practices available to ensure that the data of their employees and apprentices are guarded just like any other valuable asset.

Some cybersecurity breach–related matters have resulted in class action cases not related to ERISA, which have led to liability on an entity for failing to safeguard information of those affected by the breach.[19] The result of the liability included the entity being required to spend millions of dollars in damages, provide credit monitoring and insurance benefits, and strengthen its own internal security.[20]

Further, each state has addressed cybersecurity in a different manner, and many states require, at a minimum, notification to affected individuals when a breach occurs. JATCs are subject to these state laws and must adhere to them carefully.

Mitigating Cybersecurity and Privacy Risks

In 2020, the average cost of a data breach worldwide was $3.86 million—In the U.S., the average cost was $8.26 million.[21] This makes the U.S. the most expensive country in which to incur a breach.[22] All employee benefit funds should be prioritizing cybersecurity and data integrity because new threats are constantly being developed. Anticipating and preparing for a cyberattack will also give employee benefit funds a leg up when dealing with potential state and federal regulations on cybersecurity.

JATCs should consider performing both a cyberpractices audit and a legal policy audit to ensure that they are taking the steps necessary to prevent cybersecurity threats. These audits also ensure that a JATC is acting in a manner considered "prudent" under ERISA and complying with state law.

Training

There are several key strategies that JATCs can employ in order to minimize risks. The first is to conduct rigorous cybersecurity training for JATC staff and anyone who has access to JATC systems and data. Some studies have shown that cybersecurity and awareness training can reduce the risk of a cyberattack by up to 70%.[23] The U.S. Cybersecurity and Infrastructure Security Agency (CISA) provides a variety of cybersecurity-related resources, including free online cybersecurity training.[24]

Cybersecurity training should include the following:

- An emphasis of the JATC's responsibility to keep JATC data secure
- Review of document management and notification procedures, such as whom to alert if computer systems are not working properly and how employees should react if a computer is affected by a virus
- Instruction on password management
- Information on how to responsibly review emails and spot emailed breach attempts
- Review of the JATC social media and internet use policies
- Information on how to protect hardware containing critical data (e.g., not leaving laptops in the car, storing USB drives and devices with sensitive data in secure locations, etc.).[25]

Cyberliability Insurance

Another crucial step for JATCs to take in mitigating exposure to cybersecurity threats is to obtain cyberliability insurance. Cyberliability insurance policies will likely provide for coverage to help mitigate loss from a cyberattack. Policies can also help JATCs pay for legal fees, forensic expenses in discovering and assessing a breach, system restoration costs, identity protection for victims, and other fees or expenses brought forth because of becoming a cyberattack victim.[26]

When reviewing cyberliability policies, JATCs and their legal counsel should specifically look to ensure that coverage for social engineering fraud/cyberdeception is included. Depending on the carrier, social engineering fraud/cyberdeception coverage may not be included in a base cyberliability policy but may be available as an add-on for a fee. Further, JATCs and their legal counsel must be aware of the coverage limits for every type of breach and remedial action provided in their policies, and they must work with their insurance providers to stay on top of new threats and ensure that their policies cover those threats.

Evaluating Vendors

JATCs that use outside vendors, including providers of online courses, should ensure that these providers are securely housing JATC data they may hold. At a bare minimum, JATCs should verify that the service providers hold a cyberliability insurance policy and have cybersecurity measures and policies in place that are regularly implemented and updated. For a more robust evaluation of vendors, apprenticeship programs should establish minimum cybersecurity standards for all service providers holding valuable apprentice and JATC data. JATCs also should require all vendors to verify that those standards are being met prior to engaging in the services.

Other Proactive Measures

JATCs may want to consider hiring a cybersecurity expert or a cybersecurity audit firm to identify weaknesses in their existing infrastructure. Further, drafting and adhering to strong cybersecurity policies that include backup procedures, password management, security software maintenance and inventory tracking are effective methods to preserve the integrity of the data the JATCs continue to use and rely on every day.

Incorporating systems that limit exposure from remote work environments, such as installing a VPN for remote access, ensuring all videoconferencing applications are secure and password protected, and installing data permission policies to ensure that only those employees required to access sensitive data have access to such data are important proactive measures to take.

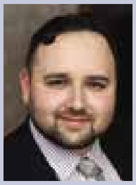
Conclusion

In the ever-evolving field of cybersecurity, the bad actors are becoming more and more sophisticated in the methods they employ to steal from and cheat their victims. The only effective way to prevent a JATC or organization from becoming a victim is to be purposeful in prioritizing cybersecurity and preservation of privacy.

Endnotes

1. "Phish in a Barrel: Hunting and Analyzing Phishing Kits at Scale," Cisco, October 31, 2017. See https://duo.com/blog/phish-in-a-barrel-hunting-and-analyzing-phishing-kits-at-scale. Accessed December 23, 2020.
2. "Flexibilities Available for the Delivery of On-the-Job Learning (OJL) and Related Instruction (RI) by Registered Apprenticeship Programs (RAPs)," *U.S. Department of Labor (DOL) Circular 2021-01*, December 16, 2020.
3. "What is Spoofing?," forcepoint.com, www.forcepoint.com/cyber-edu/spoofing#:~:text=Spoofing%20is%20the%20act%20of,Name%20System%20(DNS)%20server. Accessed December 28, 2020.
4. Ibid.
5. Ibid.
6. Josh Fruhlinger, "What is phishing? How this cyber attack works and how to prevent it," CSO Online, September 4, 2020. See www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html. Accessed December 23, 2020.
7. Ibid.
8. Ibid.
9. "Social Engineering Fraud Endorsement Coverage Highlights," Travelers, www.travelers.com/iw-documents/professional-liability-insurance/CP-8697-social-engineering-fraud.pdf. Accessed January 1, 2021.
10. Ibid.
11. Josh Fruhlinger, "Ransomware explained: How it works and how to remove it," CSO Online, June 19, 2020. See www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html. Accessed December 23, 2020.
12. Ibid.
13. "Definitions of Funds Transfer Fraud," Law Insider, www.lawinsider.com/dictionary/funds-transfer-fraud#:~:text=Funds%20Transfer%20Fraud%20means%20the%20unlawful%20taking%20of%20Funds%20from,Insured's%20account%20and%20to%20transfer. Accessed December 3, 2020.
14. *DOL Field Assistance Bulletin* 2012-01.
15. 29 USC §1103.
16. 29 USC §1104(a)(1)(A).
17. 29 USC §1104(a)(1)(B).
18. *Leventhal v. MandMarblestone Group LLC*, 2020 WL 2745740 (E.D.Pa. 2020); see also *Bartnett v. Abbott Laboratories*, 2020 WL 5878015 (N.D.Ill. 2020).
19. See *In re Premera Blue Cross Customer Data Security Breach Litigation*, 2019 WL 3410382 (D.Or. 2019).
20. Ibid.
21. "How much would a data breach cost your business?" See www.ibm.com/security/data-breach. Accessed January 1, 2021.
22. Ibid.
23. Mark Williams, "Infographic: 10 statistics that show why training is the key to good data protection and cybersecurity," Pensar, May 15, 2018, www.pensar.co.uk/blog/cybersecurity-infographic. Accessed December 23, 2020.
24. "Cybersecurity Training and Exercises," CISA, www.cisa.gov/cybersecurity-training-exercises. Accessed December 27, 2020.
25. "Cyber Security Training for Employees", Travelers Risk Control, www.travelers.com/resources/cyber-security/cyber-security-training-for-employees.
26. "7 Key Coverage Elements of Cyber Liability Insurance," *R&R Insurance Blog,* www.myknowledgebroker.com/blog/business-insurance/7-key-coverage-elements-of-cyber-liability-insurance/. Accessed January 1, 2021.

bio



Jason Kotlyarov is an associate attorney with Germaine Law Firm, PLLC, where he works with apprenticeship and other multiemployer funds to help them navigate challenges related to regulatory compliance with the Employee Retirement Income Security Act (ERISA), COVID-19, cybersecurity, litigation, Department of Labor regulations and other issues. He holds L.L.M., J.D. and B.S. degrees from the University of Missouri-Kansas City.