The Rundown podcast transcript for IT Project Monitoring Reported titled ***3 Year Summary of Security Controls in Selected State Agencies*** – Released February 2020

Brad Hoff, Host and Recruiting and Training Manager: [00:00]
From the Kansas Legislative Division of Post Audit, this is The Rundown. Your source for news and updates from LPA including performance audits recently released to the Kansas Legislature. I'm Brad Hoff. In February 2020, Legislative Post Audit released a report that compiled three years' worth starting in January 2017 through December 2019 of information technology audits and answers the question of whether state agencies adequately comply with significant information technology security standards and best practices. I'm with Alex Gard, principal IT auditor at Legislative Post Audit who worked on this three-year summary report. Alex, welcome to The Rundown. Thanks for taking the time to discuss the report's findings with me.

Alex Gard, Principal IT Auditor and Supervisor: [01:00]

It's great to be here, Brad.

Brad Hoff, Host and Recruiting and Training Manager: [01:02]
So, before we start discussing the report's findings and what the audit team found in the last three years of these IT security audits, talk a little bit about the role of the IT audit team at Legislative Post Audit and how IT audits are selected.

Alex Gard, Principal IT Auditor and Supervisor: [01:23]
Sure. As your listeners may be aware of Legislative Post Audit conducts performance audits of specific topics of interest to legislators and those topics can range anything from like school funding, Medicaid, animal welfare, STAR bonds, you name it. The IT audit team is a specially focused group, within our office, here at Post Audit, that conducts IT security and IT project monitoring audits. So, in terms of how we select agencies for audit, our team gathers data from all state agencies about their different information systems that they have. We take that information and a few other factors such as maybe previous audit results or known security issues and then use that information to select agencies for audit.

Brad Hoff, Host and Recruiting and Training Manager: [02:14]
Now I know when Legislative Post Audit releases IT security audits, the individual

ones, those are confidential because releasing that information could jeopardize an agency's IT security. Now, this three-year summary report is public because while it provides an overview of the problem areas, it doesn't necessarily tie weaknesses to a specific state agency. So, in the last three years, how many state agencies did you audit and what specific areas in IT security did you evaluate?

Alex Gard, Principal IT Auditor and Supervisor: [02:55]
So, between 2017 and 2019, we audited 19 different state agencies and audited several different areas. So, we analyzed both more technical type of areas like account security, which would be your password type settings or your boundary and network controls, which is a fancy way of saying basically, firewalls. And then also some less technical areas like providing security awareness training to staff. So, for most of the agencies, we also selected a subset of controls and evaluated a specific agency system that was reported to hold sensitive data. So, while there has been some fluctuation in the areas over the years, many of the areas were audited in all three years.

Brad Hoff, Host and Recruiting and Training Manager: [03:45]
The report mentioned several statewide initiatives that were aimed at improving the state's information security. Explain a few of these initiatives and what they hope to accomplish.

Alex Gard, Principal IT Auditor and Supervisor: [04:00]
So, the two big ones that immediately come to mind are Governor Brownback's 2011 executive order and the 2018 Cyber Security Act. So, taking the executive order first. Governor Brownback, back in 2011, initiated a centralization of IT for the state. And so prior to that order, state agencies took care of their own IT issues and then this order essentially really required all IT directors, with a few exceptions, at agencies that are in the executive branch to report to one central person, known as the executive, basically like chief information technology officer. Now with respect to the 2018 Cyber Security Act, that act contained several important pieces. First, it created this state's information security office as a stand-alone agency. So, that was a big deal. It also permitted that office to charge fees for security related functions and provided guidance to agencies on how they could pay for those fees and then the last big piece it underscored that agency heads or chief executives at these different state agencies remain responsible for their organization's security posture. There are a few other minor things that it did, including requiring those chief executives to take other steps, like ensuring that their agency had a security program and also maybe participating in like an executive leadership type of security training. One caveat I did hint at earlier, this act does apply to most executive branch agencies, but some agencies were exempted from the act, including any kind of elected offices like the Attorney General's office; KPERS, which is the retirement, the agency that manages state, retirement funds; and universities were also exempted.

Brad Hoff, Host and Recruiting and Training Manager: [06:14]
Now, one of the major findings of the report is more than 50% of the audited agencies -- so, the report says 11 of the 19 agencies did not substantively comply with the applicable IT security standards and best practices. Talk about the methodology

that the team used to measure whether an agency was compliant or not. And then that report also talks about agencies failing the compliance test. What does it mean when you say an agency failed the compliance test?

Alex Gard, Principal IT Auditor and Supervisor: [06:55]
That's a great question. Agencies failing an audit or really not substantially complying with IT security standards really boils down to a couple things. What types of findings the agency has and then how widespread those findings are. So, how many areas are the finding spread over? So, agencies that have significant findings or findings across a good number of areas are much more likely to wind up having failed an audit.

Brad Hoff, Host and Recruiting and Training Manager: [07:28]
I think it's also important to note that the IT audit team, you're actually on-site at these agencies. Typically, what's the average length of stay, if you will, at these agencies? How many days are you on-site observing, asking questions, and looking at their security protocols?

Alex Gard, Principal IT Auditor and Supervisor: [07:54]
So yeah, we actually do go on-site to these different agencies, whether they're located here in Topeka or elsewhere throughout this state. We have refined our on-site process over the years to where now essentially we are on-site for a week, five business days - Monday through Friday. In some instances we're able to finish a little bit earlier, but it's almost usually between four and five days on-site where we actually, you know, talk face to face with the people that are in charge of putting these controls in place, talk face to face with the people that are running the processes so that we get a better idea of kind of how things work and then why they work that way.

Brad Hoff, Host and Recruiting and Training Manager: [08:38]
The report includes a figure that shows the number of findings across all 19 agencies by a specific IT control area and then the severity of what you found. So, the top two areas in the critically high category were vulnerability remediation and incidents response or continuity of operations. So, what exactly is vulnerability remediation and what do you mean when you say incident response or continuity of operations?

Alex Gard, Principal IT Auditor and Supervisor: [09:14]
Alright, so, vulnerability remediation, I'll take that one first. That really can be broken down into two main pieces. 1) Scanning and 2) patching. And those really work hand in hand. So, kind of as a background when they, whether they're known or not, software is often issued with holes and that can allow an attacker to access or modify a computer or its data. So, every so often the company that issues that software will put out fixes which are referred to as patches in the industry. And those patches will close those holes or make them a lot more difficult to exploit. So, patching is really just kind of, a shorter way of saying, updating your software with a security patch. We've used scanning then as the act of using some kind of a software tool to determine whether a computer software or a computer environment has all the fixes in place or if there are patches out there, fixes out there that have yet to be

applied. So, it kind of, you can think of it this way, it's kind of like a screen on a window. So, if you don't want bugs inside your house, you have to first kind of check it occasionally to ensure that something hasn't put a hole in your screen and then you know, if there are holes, that you fix those. Getting to the other part of your question about incident response and continuity of operations. These are really the plans that you want to have in place for when something bad happens. So, incident response primarily deals with events that would be classified as security incidents. So, things like ransomware infections or accidental releases of data or a stolen computer. Any of those could all be considered incidents. Continuity of operations then deals with something that's extremely large in scale. Those type of events that might affect an agency's ability to operate. So, here we're talking about things like major weather events like tornadoes or floods or like significant disruptions like a network outage, things like that. The last thing you want to do during an emergency is figure out what you're going to do during that emergency. You know, it's the same reason that we have fire or tornado drills.

Brad Hoff, Host and Recruiting and Training Manager: [11:49]
Now another one of the points that the report makes is that the security findings that were summarized in this three-year report are similar to those in previous summary reports. Now, even though LPA doesn't necessarily audit the same agencies, it seems like there's a consistent theme that you guys are finding across these three-year summary reports. Talk a little bit about what the takeaway from that is.

Alex Gard, Principal IT Auditor and Supervisor: [12:19]
Yeah, so these are the same types of things that we've found over and over again with agencies. Many of these issues, you know, that we have identified or are fundamental and they're not new. That's the main kind of underline as these are not new issues. We're not talking about cutting edge technologies here-things that have come out in the past few years. We're talking about some basic IT security controls and basic computer hygiene. So, it really just shows that the state has a ways to go.

Brad Hoff, Host and Recruiting and Training Manager: [12:53]
Talk a little bit about what the audit team found were the main reasons for this lack of compliance in some of these security areas.

Alex Gard, Principal IT Auditor and Supervisor: [13:04]
So, there are really two fundamental causes that stood out when we looked at this and the first, really being kind of inadequate resources and then the second, really being lack of proper top management attention. So, inadequate resources, by that we mean both kind of staff, not enough staff to do the job and then not enough maybe dollars to throw at the problem. Several agencies that we looked at had staffing issues, including some relatively large agencies, which was a little surprising to us, positions, you know, sometimes remained vacant for months at a time, duties sometimes being transferred to other staff, which then led to those staff doing so much that that some basic security activities ended up being dropped. By inadequate management attention, we really mean one of, one of three things. First, it could just be ignorance. Really, top management is ultimately responsible for that

organization's IT governance and compliance with standards, but sometimes new agency heads are unaware of these responsibilities as they turn over and come into the job. Sometimes, it's inconsistent or unmonitored expectations. So, agency management sometimes overestimates the effectiveness of some of its controls or underestimates or risks associated with making changes or not implementing controls. Or in some cases, management may continue to rely on controls that worked for an environment with one set of staff and then when staff turns over or positions become vacant, they continue to rely on those controls without re-evaluating whether they need to add some additional because there aren't enough staff to do it. So, the last, you know, the last piece, for inadequate management attention really is just kind of not being security focused. So, and this is a little bit trickier to kind of nail down, but you know, by not being security focus, we really mean kind of either being slow to implement controls. So, we're telling you about these controls they need to get implemented or your internal security people are telling you about controls you need to get implemented and you say, yeah, yeah, we'll implement those in six months kind of thing. Well, you got to accept that if anything happens before you implement it you knew that there's a potential risk. I guess you have to own that risk. Sometimes management may decide against implementing security controls for business reasons. There's a lot of talk in kind of the IT world that there's a constant power struggle, for lack of a better word, between how much security is enough versus business still really needs to function. And so oftentimes, there's a trade off if you increase security, it can negatively impact business operations. And so sometimes, management might decide against implementing a security control for that reason. And then sometimes, you know, we actually found, and this was a little unexpected, we sometimes found that [the] agency executives exempted themselves from requirements.

Brad Hoff, Host and Recruiting and Training Manager: [16:47]
Talk about some of the more significant or most common security weaknesses that the audit team found from these agencies that you looked at in the last three years and why they are important to fix.

Alex Gard, Principal IT Auditor and Supervisor: [17:02]
I've already mentioned scanning for software holes and patching those holes and why that's important. And we covered incident response and continuity of operations. So, in terms of a significant findings, the biggest one I want to highlight and important is providing security awareness training to employees. This is absolutely critical. So, employees are the agency's last line of defense against intrusion and can unknowingly circumvent technical IT controls that otherwise would protect the agency and its data. So, think of it like this. You can have the most sophisticated alarm system on your house, guard dogs, like James Bond style retinal scanners, mote with alligators, flame throwers, what have you. You could have all of that, but you know, if your grandmother or your four-year old invites the suspicious looking cable guy in, you know, those controls aren't worth a thing, so your goose would be cooked. That's why agencies really just need to absolutely train their employees on IT security awareness and start building that culture of security from the ground up. In terms of other common findings, we test many different types of things. So, access controls, physical data center, security, data protection. I guess just

to give you a little, a little taste, a few examples. You know, we found issues with agency passwords not being long enough or not being complex enough. We found issues with the physical security surrounding an agency's data center, which is really where an agency's data lives, on its servers there. We found issues with agencies' asset inventories of IT equipment, so their lists of computers and tablets and things like that being incomplete or missing items from that. And we found, you know, issues with agencies' processes for destroying sensitive data or folks basically pitching things that should be shredded into the regular trash. So, yeah, it seemed like almost for every single thing that we tested, over the years we've found at least one agency that's had a problem in those areas.

Brad Hoff, Host and Recruiting and Training Manager: [19:31]
The audit team also found a significant number of problems that exist within agencies' specific IT systems that maintain or process confidential information or very sensitive data. So, talk about some of the examples that the audit team found in this area.

Alex Gard, Principal IT Auditor and Supervisor: [19:53]
Some of the problems for systems are not so different than those we found in an agency's IT environment as a whole. So, for example, locking accounts that if they incorrectly enter a password would be a good control against somebody trying to guess your password, but also like computer programs set to just automate that effort. Right along with that, it is kind of widely acknowledged that when user passwords are longer, they're tougher to crack, tougher to guess. So, we've found agency's systems that did not lock accounts out so you can try as many times as you wanted to guess a password and some systems actually even allowed one character passwords, which just makes the list of possible passwords that much shorter. We also found problems in controls that we checked only in the system area and not in the agency's IT environment as a whole. So, things like, programmer's writing and testing code in the live production environment. So, in non-IT speak, you know, programmers are basically adding new features and everything on the system as it is running. So, if anything goes wrong with that, it could bring the entire system crashing down. A third example is that some agencies weren't backing up their systems. So, if anything went wrong, whether it's a power surge, you know, ransomware, catastrophic weather event or even like, like I mentioned just a minute ago, the programmer's writing and the actual production environment, if something went wrong, agencies risk not only losing their system temporarily, but without that backup, possibly losing some of that data permanently.

Brad Hoff, Host and Recruiting and Training Manager: [21:49]
So, the audit team identified deficiencies [and] weaknesses across these 19 agencies that you looked at in the last three years. What type of follow up will the IT audit team, perform, carry out to ensure that these deficiencies and weaknesses are addressed, resolved, and that improvements where necessary are made?

Alex Gard, Principal IT Auditor and Supervisor: [22:17]
So, our team has a standard follow-up process with agencies. It generally happens a year following their audit. So, for agencies issued or agencies that were audited in

2019, we'll be following up with them in 2020. During that process, we contact the agencies and determine really what kind of progress they've made on the findings from the prior audit. We then summarize and report that information to our Post Audit committee, who may have additional questions for us or for the agencies themselves. And then one thing to keep in mind is that we re-evaluate at the end of every year, kind of, who is on deck, if you will, or set up to be audited. So, agencies that don't do as well or have a greater number of findings or more significant findings are much more likely to come up for an audit again sooner then those agencies that have a little bit cleaner results.

Brad Hoff, Host and Recruiting and Training Manager: [23:28]
Finally, what is the main takeaway of this report?

Alex Gard, Principal IT Auditor and Supervisor: [23:32]
These findings are really important. So, the state could face, you know, significant consequences if an agency's poor security controls are exploited. Whether that's in the form of a disruption, of an agency's mission critical work, all of a sudden they're no longer able to kind of do the things that makes them them, whether that's kind of financial impact and the form of either, you've seen breaches out there and then companies or states or whoever saying "Hey, we'll offer free credit monitoring." Well that's not, I mean, that's free to the people whose data got exposed, but it's not going to be free to the person that has to pay for that. So, and that can be expensive or you know sometimes there are other legal liabilities or penalties depending on the type of data, you know, it could be in the form of fines, whether it's from the federal government or abroad. So, now all that being said, despite the state having kind of taken some steps to strengthen security as we laid out, towards the beginning, there is really still a lot of work to be done. So, we really just kind of hope that by helping agencies identify some of these security weaknesses, they can start addressing those gaps and start making Kansans data more secure.

Brad Hoff, Host and Recruiting and Training Manager: [25:02]
Alex Gard is a principal IT auditor at Legislative Post Audit. He helped compile a three-year summary report from January 2017 to December 2019 focused on whether state agencies adequately comply with significant information technology security standards and best practices. Alex, thank you for taking the time to walk me through the report and visiting The Rundown.

Alex Gard, Principal IT Auditor and Supervisor: [25:28]
Thanks a lot.

Brad Hoff, Host and Recruiting and Training Manager: [25:29]
Thank you for listening to The Rundown. To hear more podcasts, subscribe to us on Spotify or Apple podcasts. For more information about Legislative Post Audit and our audit reports, visit www.kslpa.org and follow us on Twitter @ksaudit.

be acknowledged as the source of the information. Listeners may not use this information to imply LPA endorsement of a commercial product or service or use it in a way that might be misleading.