WIPFLI

IT examination hot topics – The latest trends
Webinar questions and answers
March 24, 2021

1. Any trends for regulators for reviewing controls over the use of machine learning, and other AI components?
    a. Not directly that we have seen. As with any service, we recommend concentrating on the vendor management aspects (SOC reports, etc.) for now.
2. Is an IT AUDIT risk assessment different from an IT Risk Assessment?
    a. Yes, it is. While we have had clients use an overall IT risk assessment (often used with GLBA as well) to determine the scope and frequency of an IT audit, it can be difficult to match everything up to a typical IT audit scope. We would recommend a separate risk assessment if you haven't performed one in the past.
3. And is are these topics focus for OCC, DFI, or FDIC and/or all of the above.
    a. This webinar is meant for all financial institutions, regardless of the overseeing agency. Our team follows FFIEC standards, which apply to all agencies.
4. Have you seen change detection as a requirement? very hard to do...
    a. We agree this is difficult and can be expensive, though we have not yet noticed this as a requirement. For financial institutions that are FDICIA/SOX compliant, this becomes more important — particularly if you are running financially significant applications in-house (and especially if you are developing those applications). You want to be able to provide an accurate and complete population of significant changes to the financially significant applications (like application or database updates). If your regulators or your financial statement auditors are not pushing for this yet, I would not consider it a requirement.
5. For Change Management Policy - what extent of changes should be identified in the policy? Major vendors? Servers? Employee access changes? How granular should we get in the policy?
    a. The policy should explain what is considered a change and what is not considered a change. Major changes (server replacement, new application/service, core conversions, etc.) should be documented each time they are done. The policy can contain information/procedures for basic/common changes like employee access, patches, etc., so they do not need to have written documentation every time they are performed (try to make sure there is some logging/reporting that can be referred to for them).
6. What documentation would you get from a third party that performs change management for you?
    a. You can still use the same methods as if you were performing change management in-house. Your vendors should have a plan for implementation as well. The change should still have an approval process, testing procedures, a plan for backout, etc. Make sure your vendor is aware of your requirements to ensure they are providing the proper documentation.

7. What are you seeing for Cybersecurity Assessment Tools being used/what do you recommend? CAT, ACET or InTREx?
    a. As with #9 below, the spirit of the tools is to have a framework to measure cyber readiness. We see CAT used universally, with credit unions using the equivalent ACET tool. We've heard that InTREx is going to replace CAT, but at this time InTREx is still more a methodology for regulatory agencies to perform exams rather than a framework for the institution to follow. It will still incorporate the same guidance as before but is a methodology for how they conduct their exams.
8. When you stated reported to the Board, does that mean just presented and reviewed or do they have to have an approval?
    a. There should be acknowledgement that the Board received the reports and has reviewed and accepted them.
9. What about CSF? Is CAT really mandatory? Or is it mandatory that we use a framework of our choosing?
    a. The spirit of the requirement is that a framework is used to measure cybersecurity readiness. The NIST Cybersecurity Framework (CSF) would work as well as CAT or ACET.
10. At one point can the board say "We are as mature as we're going to get for our size"
    a. We recognize that many of our clients are small, many are in rural communities, and status quo is the way things are done. But we don't believe it's a good idea to say you are "as good as you are going to get." There is always room for improvement. CAT/ACET are meant to be reevaluated on a regular basis. Sometime in the near future there may be some new technology that makes moving to the next level, be it evolving or even higher, affordable and obtainable. While it is okay for the Board to accept where you currently are, never say never when it comes to being able to improve more down the road.
11. Is reporting the CAT results to the board considered a requirement or a best practice?
    a. While the regulators have never specifically stated it is a direct requirement, they definitely expect that you will present the results to the Board, and your IT auditors will expect that as well.
12. There is a presentation by the Fed on March 31 as well.
    a. Excellent news! The more information we can gather on this, the better!
13. Is a Yubikey considered a multifactor component?
    a. Yes, it's a good additional factor. It is "something you have" — the device that holds the token. So you would still need a "something you know" and/or "something you are" to have full multi-factor authentication.
14. What is the best practice to handle remote access for furloughs?
    a. Technically speaking, they are still employed by the financial institution and would still be bound to the AUP, remote access requirements, etc. If an employee is furloughed and will no longer require access for an extended period of time, we recommend access for that employee be disabled. If that employee's emails are important, consider forwarding their mail to another employee or allowing another employee access to their mailbox. The employee's access can be reenabled when they return to work. You may want to determine whether equipment should be collected during that time or not, as well.

15. What specific SIEM alerts and notifications should we have setup?
    a. Each SIEM system is different, but depending on how you want to be alerted for remote access, you could have it configured to alert on successful login of a remote employee, unsuccessful attempts and lockouts, attempts after typical hours (or assigned hours), etc. You can get as granular as the system will allow or as you would like to get notified — "every time a file is accessed" might give you so many notifications, you might pay less attention altogether, so make sure it is set up to accommodate what you are looking for and can handle.
16. Can you give example of what most are using for MFA when working remotely?
    a. We typically see security tokens — usually app-based "soft tokens" such as RSA, MaaS360, and Duo — or text-based codes. There are some remote solutions where a preinstalled certificate on the remote machine functions as that authentication factor (Cisco AnyConnect and SonicWALL's VPN come to mind). Essentially, if your remote solution does not have a baked-in secondary factor (generally in the "something you have" category), you need to add that layer.
17. While a lot of businesses are going back to the office many are not. Any points specific to expanding a permanently remote work staff? We all scrambled for short term security but it is turning long term.
    a. This is an excellent point. This has turned into a long-term situation and, in many industries, possibly even a permanent one. You first need to ensure your risk assessments and IT strategic plans have been updated for this. We know some financial institutions had temporary policy exceptions, so those may need to be permanently updated. You need to ensure the controls implemented get you down to your acceptable risk levels. For any gaps, other controls should be considered.
18. How long until MFA is required for all logins including local, not just remote access?
    a. This is a great question. From an internal network perspective, I'd start thinking about requiring MFA on high-risk accounts, such as administrator accounts, first. In some states, this is already a requirement; it may go national during this presidential administration.
19. What are your thoughts on Password manager applications like LastPass or Dashlane?
    a. The best way to answer that is by telling you that Wipfli uses a password manager application for its 3,000+ employees. We are absolutely in favor of using password applications. We all constantly hear from the users that there are way too many passwords to remember. And we know that in those cases, users ***will*** write them down (we've seen passwords written on sticky notes, calendars, rolodexes, pads, etc.). Just make sure you do your due diligence and appropriate vendor management.
20. For multi factor authentication, how would regulators like to see this done. Via text message to the user's cellphone number, or have a code emailed to a secondary email, or some other method?
    a. First and foremost, we'd recommend ensuring some version of MFA is used. As for the types of MFA, using an app-based authenticator or a physical token is recommended over SMS (text messaging). There is some concern about texts being compromised; however, any type of MFA is better than nothing.

21. Which was worst in your opinion SolarWinds or Exchange
    a. This is a good question. I'm not sure I would proclaim one over the other for a couple of reasons. First, we still don't know the full extent of either. Second, in both cases, compromise didn't necessarily mean it was taken advantage of. SolarWinds left a back door, but was it used on you? With Exchange, even if a shell was dropped, do we know whether it was left for later with no further compromise, or was it taken advantage of? Both are very different kinds of attacks. SolarWinds was a supply chain hack, which should have you thinking about vendor due diligence; Exchange is exploited code that was in place from Microsoft. While the Exchange compromise appears to be more actively attacked, time will tell to what extent.
22. What specific control questions should be evaluated when auditing a Hosted Exchange Servicer
    a. We recommend starting by requesting information about when the provider patched the systems and whether or not they have performed testing to see whether the server(s) hosting your information had signs of compromise. If they do not release this information to you, review the contract agreement to see whether there are any grounds for demanding the release. If not, evaluate the integration of the servers with your internal network resources. If there is not a route for further compromise of your internal network, you may have to worry only about the hosted system. Again, contact your insurance provider to see whether you have adequate coverage and see what steps they recommend. Many providers have a forensic firm that you will be required to use. If not, you can always reach out to Wipfli for forensic investigation if you want to try to determine whether any compromise happened.
23. As a bank I worry about BEC as a result of internal exchange servers from partners sending phishing emails to my employees
    a. We agree. According to the FBI's Internet Crime Report, business email compromise was a top attack vector even before the Exchange attack. Be sure to educate your employees as such. The best way to confirm your employees' awareness is to perform email phishing tests on your employees and train, train, train.
24. We patched. Is there any concern about vendors we use that may not have patched. Revised Question: Related to the Exchange vulnerability, is there any concern about vendors we use that may not have patched.
    a. Yes, there is reason to be concerned if you suspect vendors are vulnerable to this. This is a good time to remind everyone to not send sensitive information via email and to always use secure file transfer systems. Also, hold your vendors accountable. Ask them what they are doing to fix the issue and follow up with them. If they cannot deliver, it may be time to look at other solutions.
25. And there are self-use tools to help identify if you were compromised.
    a. Microsoft's blog on the issue — the link is provided in the slides — contains information on the tools they created for detection. You'll find this under the "*Can I determine if I have been compromised by this activity*" section a little more than one-third of the way down the blog: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.
26. You can contact your ins. co. to get Wipfli as the approved vendor...we did.
    Revised question: Can you contact your insurance company to add Wipfli as an approved vendor for forensic investigations?
    a. You can request your insurance company add Wipfli as an approved vendor. Some of our clients have had success doing this. We have a fantastic forensic team, so we appreciate the vote of confidence from those who have added us as an approved vendor.

27. It still is not clear to me what has been exploited or what information they received and what/how/if they are going to use it.
    a. This is regarding the Exchange hack. The exploited code allows attackers to insert code that will allow remote access to the system and network. From there, it is up to the attacker to decide what they want to gain access to, attack, steal, or other activities they wish to perform. Essentially, they can use the privileges granted by PowerShell to do just about whatever they want.
28. Can you explain the PaaS again, i missed what you said?
    a. We were able to address this in the question session at the end of the webinar. If you have more questions, please feel free to reach out.
29. Will an offline version of this be available for download at some point? Very good info and would like to re-listen to the extra details that were not written out in the slides.
    a. Yes! You will be able to re-watch this presentation. Please allow a couple of days, and it will be uploaded to our website.
30. Will we get an email regarding the Fedline solution session if we are on today's webinar?
    a. Yes! If you received an email invite to this session, you will receive an invite to our IT Roundtables, where we will present this topic in more detail.