I'll Tell You What You Need to Know

While walking past the president's office, he sees and summons you into his office and asks if you can fix the printer on the back wall. After astutely seeing the printer's status panel is indicating "Out of paper," you load paper and *voila*, it prints. "*Hey, you're pretty good at this technology stuff. Our last exam said we had to appoint an Information Security Officer that isn't part of the IT Department. That will be you.*" The president gets the Board of Directors to formalize the role and title, and before you know it, you are officially the bank's ISO (Sorry, no raise, but you do get new business cards! Wahoo…).

You settle into your new role (that is nestled atop previously assigned responsibilities, but that's outside the scope of this blog… sorry) and quickly learn that, as ISO, you are expected to oversee various technology-related security functions. Those include antivirus, firewalls, log management, patch management, backups, and various other systems. You're excited to grab the reins and make a difference, which takes you to visit the manager of the IT department. The manager is thrilled to see you, too…

"*Congratulations, I guess you get to do the annual information security training for the bank. Here's a stack of vendor due diligence reviews for you to complete.*" Suddenly, the meeting isn't going the way you envisioned, and you semi-confidently respond with "*I also need to oversee the security systems, such as antivirus, patch management, log…*" to which the manager cuts you off and says, "*I'll send you a copy of some reports. I'll send you what you need to know. Now I must get on a conference call. Good luck!*" It then it sinks in; you really aren't sure what YOU need to know as the ISO or where the dividing line is between the ISO role and that of the IT department.

Sure, the above is a fictional dramatization, but it mirrors the basis of many discussions/arguments in banks (and other organizations) across this land. It should be an easy topic to answer, but since it involves the volatile mix of humans, technology and government guidance, "easy" isn't realistic. The following are common questions that novice ISOs often struggle to find answers:

Does regulatory guidance offer any answers? Yes, and that's a good place to start. In the FFIEC IT Examination Handbook – Information Security (2016) it is noted, "*Management should designate at least one information security officer responsible and accountable for implementing and monitoring the information security program.*" and further "*To ensure appropriate segregation of duties, the information security officers should be independent of the IT operations staff and should not report to IT operations management.*" Summarized, the ISO is responsible for implementing and monitoring the bank's information security program (ISP), but is separate from IT administrative duties. To adequately monitor the ISP, the ISO must have visibility to any and all security-related functions. This includes firewalls, antivirus, patch management, log management, backups, etc., since these are all defined within the information security program (if they are not in the program, you should add them, pronto).

But what is MY responsibility as ISO and what is the IT department's? Let's look at this from a different perspective. If the IT administration functions at your bank are outsourced, you should have an agreement in place between the bank and the third-party that details the responsibilities of each. In that instance, you would likely expect the IT vendor to perform the day-to-day administration and monitoring, but the bank would still be responsible for monitoring the vendor and receiving sufficient reports and information to ensure they are appropriately performing assigned duties. That is essentially the same model the ISO should expect from an in-house IT operation. Whether IT administration is performed within the bank or by a third-party, the ISO must have adequate visibility into each function to receive assurance that those functions are being performed sufficiently to protect the confidentiality, integrity and availability of the bank's information assets.

That makes sense, but I still am unsure what I NEED to know. Let's look at an easy example: antivirus. As ISO you NEED to know that all workstations, laptops and servers have current antivirus software installed, functioning and up to date. Also, if any of those systems were to encounter malware and generate an alert, the ISO must receive prompt notification of the event. That does not mean only receiving a monthly report, or even a weekly report. Weekly and monthly reports are adequate for general status of the antivirus systems, but not for alerts. Now apply this same logic to other systems and functions; firewall monitoring, backups, IPS, patching, etc. If you are still unsure, put each of the security systems/functions to this test: Imagine having an auditor or examiner sitting across the table from you, asking what your visibility to any security system might be, such as "*So, you are the ISO. Would you know if last night's backup failed?*" or "*Do you know the current status of this month's Microsoft patches being deployed across all your systems?*" If those questions make you queasy, then you probably need more visibility on the given system to provide adequate oversight.

Putting it delicately, my bank's IT manager has a "strong personality" and it is hard to get him/her to take my requests seriously. First, you should understand that regulations and best practices are behind you. Arm yourself with backing regulatory guidance, past audit or exam findings, and let him/her know you are tasked with ensuring the bank is secure and in compliance. The ISO's job is to see the big picture and evaluate the security risks, whereas the IT department is to operate and administrate the IT environment. Ultimately, all should be on the same team and should be working together. If that doesn't get their attention, then you need to find someone far enough up the food chain to get the IT manager's attention. That may require that you discuss your concerns with the president that appointed you to the position. Culture is usually driven from the top, so if the president supports information security, your points will be well-received.

Full disclosure – if I get all those reports and information, I am not sure I know what I should be looking for. Well, that is a challenge. Not that it will make you feel any better, but you are not alone. You'll have to get over that hump, but it doesn't all have to occur at once. Pick one weak area and focus on gaining competency on it. Let's say you start with antivirus. Ask to sit down with the IT person (or a webinar with the IT support vendor) that is tasked with ensuring antivirus is installed and operating on all systems, then have them explain how they monitor it, the alerting options, and what those alerts generally indicate. Go into that discussion with questions written down in advance, so you maximize the use of your time and theirs. Get comfortable with a topic area, then pick another; rinse and repeat.

It sure would be nice if there was some place I could get unbiased training on what an ISO needs to know! Funny you should ask that (and ignoring for the moment this question was shamelessly inserted by an instructor at 10-D Academy…). We have an "Essential ISO" class that is designed for ISOs needing a knowledge foundation and a subsequent "Advanced ISO" class. These are also useful for other management within the bank that need or want training to help secure their bank and to excel at the next exam. For more info go to www.10dsecurity.com and click on "Academy."

Are there any other options or factors to consider when deciding responsibilities shared between the ISO and IT department? Ultimately, the bank needs to ensure their assets safe and secure. Turf battles can result in insufficiently protected customer information, so don't let that happen. That may mean you will need to let, perhaps temporarily, the IT department retain more control of a system. Or it may mean there are instances where the ISO is the most technically competent to administer a system and therefore retains administrator access. If either of these are the case, have better-than-average transparency and reporting to an IT Steering Committee and senior management, otherwise you may be criticized at the next audit or exam. Also, it is wise to have a separate budget for information security (including cybersecurity). Examiners are expected to evaluate whether banks are allocating sufficient resources for information security, and this is an excellent means to provide proof the bank is doing so. Regardless whether examiners look at the budget, it is still useful to have one specifically for information security as that can be the deciding factor in turf battles ("*I'm responsible for the budget for the log monitoring system, therefore I will determine how it is used…*").

A final thought. Don't get discouraged when you have the inevitable feeling that you don't understand a topic or have control of the situation. That's quite normal, and may even be a sign that you have achieved a reasonable level of understanding your new role. Now muster up the courage, go back to the IT manager and say "*Thank you for the information you provided earlier. But since I have been assigned responsibility for the bank's information security by the Board, I am going to need a few more things. Here's my list…"* You got this.