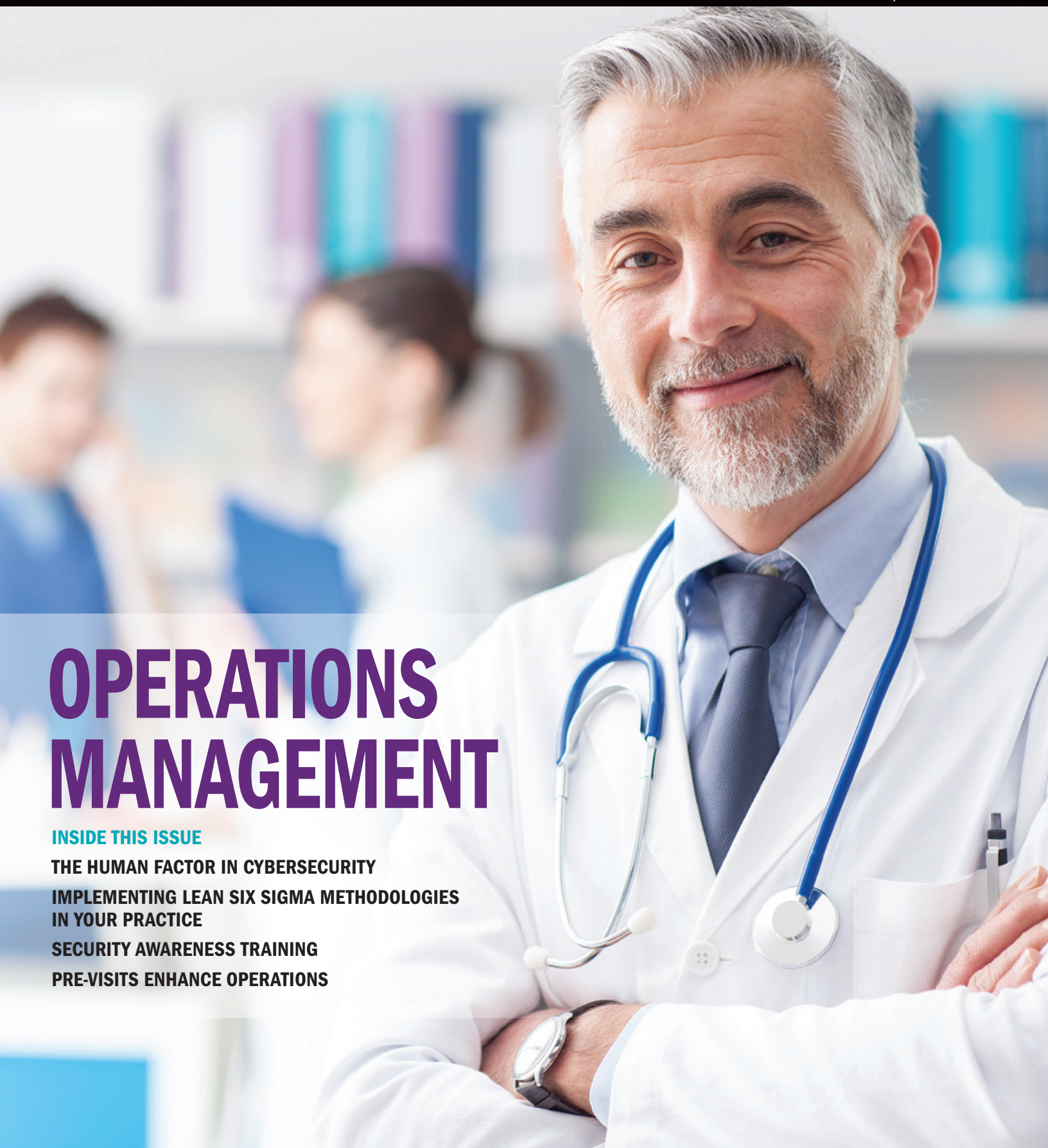
A PUBLICATION PROVIDED BY
MGMA MARYLAND

MediNews

NOVEMBER/DECEMBER 2017



OPERATIONS MANAGEMENT

INSIDE THIS ISSUE

CONTINUED FROM PAGE 7

PART 2: WAITING ROOM EFFICIENCY – IMPLEMENTING LEAN SIX SIGMA TO THE SCHEDULING PROCESS

I've always been one to try to streamline parts of my life. From childhood, I incorporated time management techniques into my daily routine and was not a procrastinator; I hated bottlenecks. So when I began to learn about lean six sigma (LSS), and ultimately go through training, I realized the LSS principles are in my DNA.

With that in mind, one day recently I took the day off of work and scheduled multiple doctor appointments. It's a pre-tax season ritual with many of us accountants. It was a small challenge getting them all arranged, but I was able to get them in a logical sequence from a geographical and time perspective. The one that concerned me the most was the 2:00, which was preceded by a 1:00 about 15 minutes away. But the 1:00 appointment was a follow-up to a procedure that would require three minutes of the doctor's time and was the first appointment after lunch. NO PROBLEM, right?

I arrived early at my 1:00, to ensure I was the first patient seen. I signed in at 12:20 and was the only person in the lobby. Another patient arrived around 12:45 and signed in and was called back before me, but I figure they have multiple doctors; I'm still first after lunch. I was called back about 1:05 and placed in a room to await the arrival of the doctor.

Numerous times I heard my doctor (who appeared to be the only doctor there) call over the paging system for assistance in the room next to me. About 1:25 I finally asked if I was going to be able to see the doctor in the next 5-10 minutes. I created a little bit of a stir in the office, especially when I found out they double booked appointments. They asked if I wanted to reschedule. No I don't want to reschedule; I took the day off of work to take care of a bunch of things. I was here 40 minutes early: for over an hour now! The doctor finally came in and saw me at 1:35 and I walked out three minutes later rather agitated.

During those three minutes I asked him why I was not seen first since I was there at 12:20 and required an insignificant amount of time compared to the other patient. He said "I just take the patients in the order they tell me to."

I walked out thinking, "What a great opportunity to implement the principles of Lean Six Sigma to the patient scheduling process". It's about making your customers happy and reducing waste. I was obviously not happy. And what a waste to make the patient with a three minute time requirement sit in the office and wait 35 minutes past their appointment time. A better solution would be to see the short appointment first while the person having a 30-minute procedure could have been seen at 1:05. Two happy patients, instead of one annoyed patient. Not to mention I was there well in advance of the other person. While implementing the principles of lean six sigma to the scheduling process, a practice could incorporate both the arrival time and the length of face time into process when patients are double booked. Implementing certain procedures and policies could streamline the scheduling process and help to eliminate waste (bottlenecks, etc.) and improve patient satisfaction.

Happy customers are loyal customers that make referrals. Annoyed ones just write articles about their experiences. ■

Security Awareness Training

A NECESSARY AND POWERFUL TOOL TO PROTECT PATIENT DATA

OVER THE PAST SEVERAL years, I've spent considerable time with clients working to develop better IT policies when it comes to things like Acceptable Use, Privacy, Security, and Incident Response. These policies are all important and necessary, because if you don't properly equip your staff with rules and guidance on the expectations for their handling of technology and by extension sensitive data, you can't expect them to act responsibly.

But this goes beyond simple drafting of policy by management and acknowledgement by staff. Policies won't necessarily educate users regarding the threats out there, or even more fundamentally, what some of threats mean to them. Moreover, policies are often stagnant. They are created to establish a guide for how people are supposed to act, but they do not necessarily speak to what a staff member might have to deal with on the most basic level of their day-to-day tasks. How is a staff member supposed to recognize a malicious email, illegitimate website, or applications that are not trustworthy? Even as an IT professional, I still run into new threats that I have to educate myself on, which means I have to continue to self-train on a regular basis.

If you look at the statistics, groups that have sophisticated and well thought out Security Awareness Training programs have fewer security incidents. This leads to real returns on investment for training products and services that really don't cost very much, especially compared to the cost and impact of a major security incident. If you avoid one incident because of awareness that wasn't in place before, the entire training program likely pays for itself. That's why a number of compliance standards mandate a Security Awareness program.

Ben Schmerler
Senior IT Risk Advisor,
DP Solutions

In this article, I'd like to discuss ideas behind developing a Security Awareness Training program for your practice.

TRAINING CONTENT

The first step, whether it is coming up with a Security Awareness Training program or designing a fully functional networked computer system, is identifying what kind of data you are working with. As a medical practice, you are most likely primarily concerned with Patient Health Information (PHI) and financial information. So any training that you would implement should keep that kind of data in mind and in context. For example, it wouldn't make sense to train on the Payment Card Industry (PCI) rules in an environment where nobody handles credit cards. However, for medical practices, general HIPAA/HITECH awareness is essential. We want staff to know the legal and regulatory rules to which the data they are touching every day must adhere.

However, looking only at compliance rules is not really seeing the forest for the trees. An end user who falls for a phishing scheme and gets hit with ransomware, or perhaps worse, unintentionally breaches information by volunteering patient information to an unauthorized user isn't necessarily lacking in awareness when it comes to the concepts of HIPAA rules and compliance. These users need a basic education in responsible use of technology.

Therefore, the content for your Security Awareness Training program must speak to practical technology concerns. Start with looking at your workflow. What applications are end users working with? Are they installed locally on the PC or are they some kind of web application? How does staff usually communicate? Is the organization involved in social media? Is web browsing a major part of work flow? Does staff work remotely? Essentially, you need to create a "menu" of training that speaks to what they actually do day-to-day.

Typically, when I put together an agenda for training, it's based on the organization's specific operations. I try to take content that's purely technical security, like how to recognize phishing emails, defining threats like malware, and explaining the role of encryption and what it means, and also toss in information about what to look out for when reading emails, browsing the web, or engaging in social media. We want the content to be broad, and not limited to a particular discipline of Security Awareness, but specific and tailored enough that the content within the training program still remains relatable.

You should also consider whether all users should get the same content or not. In some organizations it makes sense for certain users who have privileged access to special data to receive more robust trainings that speak more to specific concerns for their role.

TRAINING FREQUENCY

End users will "check out" of your training program if it's not done the right way. They will look at training as a box to check off rather than a valuable tool to improve their awareness. Our end goal is to achieve better outcomes by improving user awareness, so it is essential that staff buy in to the program. It's also important to recognize that awareness training, while important, is perhaps not the most exciting subject, and it can also be difficult to grasp depending on the specific subject matter.

So when coming up with a Security Awareness Training Program, I recommend spreading out some of the topics into a series of smaller, more digestible chunks. There are several advantages to this approach. First, this makes it much easier for end users to understand and learn. Also, individual trainings can be distinctly focused on a discipline, like technology terms or recognizing phishing emails, so that the material doesn't blend together too much. Finally, I prefer agility when it comes to a training program. The content should have several broad goals, but should be flexible enough to update the content based on new threats, changes to the organization getting training, or other general changes to the world of technology. Coming up with somewhat regular training sessions that gives a slow drip of a variety of information will create a much more aware workforce than other approaches in my opinion.

SECURITY TESTING

Every kind of awareness training should come along with basic testing. It doesn't have to be the SATs, but we do want to make sure the audience isn't zoning out on the training. Simple quizzes get the job done.

Furthermore, there are things we recommend outside of educational training that organizations can do like Phishing Testing. This is where fake phishing emails are sent to users. The simulated emails are designed to try to trick the user into responding or clicking through some kind of link in the same way a real Phishing attack might occur, but without the negative consequences. You can even redirect users who fell for the test to a landing page with tips on how to recognize that the email was not legitimate. Or you can put them into a small group to get additional basic training to reinforce and improve their awareness. One of the things I really like about Phishing Testing programs is that they speak to a current issue, something end users can relate to, and they can tie together not just awareness on Phishing but other Security Awareness concerns.

Like most things having to do with the implementation, management, and support of technology, there is no one-size-fits-all solution. My recommendation is to start thinking about your organization, what you do, and how you do it, and then develop a program of training and testing that fits practical concerns that speak to your staff, isn't overwhelming, and delivers the results you are looking for. ■

Ben Schmerler is a Senior IT Risk Advisor at DP Solutions, one of the leading IT managed service providers (MSP) in the Mid-Atlantic region. Ben works with clients to develop a consistent strategy not only for technical security, but also policy/compliance management, system design, integration planning, and other business level technology concerns. You can follow DP Solutions updates on LinkedIn or their website: www.dpsolutions.com.