NAME

Printing Over Coffee Episode 3

DURATION

22m 19s

START OF TRANSCRIPT

[00:00:11]
Hey, everybody, how's it going? Welcome to another episode of the Printing Over Coffee podcast. If you are new to the podcast, this is where we sit down with top industry experts and thought leaders to extract key insights to what you can apply to your day to day and help you solve your printing challenges.

[00:00:27]
So in today's episode, we will be covering security and compliance in how you go about protecting confidential data while meeting certain industry requirements. Now, oftentimes, security and compliance are said in the same breath as if there were two sides of the same coin. But as we know, they also are very different with different purposes and different outcomes. So Arron what can you tell us about security and compliance? What are their main differences?

[00:00:55]
Yeah, I think I have to focus on the IT point of view, security and compliance. So compliance is more regulation. I want to be compliant too software. I want to be compliant to these flips and all this stuff. Those are standard that third party are looking for from a company. Are you complying with this? I compliant with that. So it is formal, policy driven, high level. Security is more practical. It's like I need to implement my firewall and this rule I put on and certain security and its implementation kind of scenario from my point of view. So that's why I can tell kind of between security and compliance. But in a strict sense they have more or less apply to the same thing.

[00:01:45]
Right. And so from a organizational standpoint, what makes security and compliance so necessary? Why is it important for them?

[00:01:53]
Well, compliance is important for certain market. So the government have compliance for IT to come in with a certain application have to be compliance to this, HIPPA compliance. All these different things. So security is to backup compliance in that sense. I'm comply because of this. I'm comply because of that. So it is necessary, especially in IT application or some sensitive common sensitive information. Healthcare, financial. They are looking for compliance from the application or even from a person or how certain policies is running the company.

[00:02:33]
What would you say are some common misconceptions on security and compliance?

[00:02:39]
I think one of them would be a compliance only for auditing. We are only complaint because there's a requirement, but in effect, compliance and security, I'm going to use the same word, although there is a difference. But in an IT straight sense, it is to protect yourself from external hackers. Now that everything, most of the information are digitize, it is in the network, it is in your data center somewhere. If you don't lock that door properly and put protection around all this stuff, you can pay a big loss because someone can just get into your server, copy all your customer information, security, visa number, everything, and suddenly you're in big trouble. It might not happen, especially when a small company say, hey, why do I need to do this? But has your company grow more data going to be accumulating in your server and it become a very important aspect of your business to make sure you, your security and compliance up to date.

[00:03:40]
Now, what would you say to certain misconceptions like real time visibility is impossible or it's always better to block access to your system?

[00:03:52]
It is hard to do, right? So real time. Real time visibility is harder than obviously going back to do an audit trail. So like a volume printing point of view, it's much easier to have people print and then come back and say, OK, I'll allow printing. But if there's an issue, I come back and do an audit. Obviously, it's better than no security at all. There's no way to audit. But in order to be able to say

I stopped someone from printing sensitive information, that's the rule ought to apply and that also restrict access to people. And it might it might slow down your operation. So it is harder to do. It is not a misconception. Real time, it is hard to do. To add real time and efficient and therefore don't block people from working is hard to do. For instance, I'll give you an example. One of the hospitals that we do. Right. So the most secure way of printing physically is to use what we call secure pull printing. People print, you not in front of a printer, you cannot release the print jobs, so print job that never release directly. So when you print something from the workstation to a printer, you don't get the print job until you walk over to the printer, authenticate and release. Obviously, that is the best way to make sure that you in front of the printer before the printer job get released, so it won't be there lying around for people to pick up. But then in a hospital environment, every single second count. So the most expensive staff in a hospital is normally the ER Healthcare staff. Right. So the doctor do not want to spend the time even to wait for a print job. Hard to say whether that's a real issue or is it just a doctor. But anyway, the requirement is, hey, I want my print job to be there when I print and when I go and pick up the job. So what is the couple of thing that you can do? One of the thing maybe you can do is have a lock box. Printer jobs are already printed. Only this guy, key in a lock, and that's a very expensive exercise. But in the meantime, you could make it more compliance, more security by assigning the right printers so that they don't get the print job printing to the wrong printer because doctors are very mobile. So you can see that the security have created a lot of blocks, like it slows down normally people for access or easy to use, but at the same time it's necessary. Then there is some work around to kind of strike a balance. And that's one of the thing that is really hard to do.

[00:06:24]
And so what would you say is the number one reason most organizations fail to succeed when they're trying to build a secure and compliant printing environment?

[00:06:34]
I was always say planning. Just like the case I just mentioned before, right, for a doctor. If you don't plan this out and you push secure pull printing, to the whole organization and you find out rejection is going to come from the ER Department, saying, you know what, people life is at stake and you are making it very difficult for me to do my work. So then you have to compromise. So plan, survey, is part of the planning. Obviously, you've got to find out how people work, study their workflow, plan ahead, make sure the solution will work both in a compliance point of view and also from a usability point of view. And when you combine all that together, compromises have been made and then you have to sign off like any other project. Then you've got the buy in and you've got to make them understand, educate them. And then when you push out the actual implementation, you won't get any resistance because security means more work for the user. Right.

[00:07:29]
Right. And when it comes to specific road blocks like digital physical convergence, how would you overcome these type of roadblocks?

[00:07:39]
It is tough to overcome. Education. Money that you have to spend. It is a balance between cost, right? Like, for instance, I have all my printers have been five years old. That means most of them have security protocol, the printing protocol is not secure. The printer doesn't have support, secure pull release. So do you want to change the whole fleet? And that's going to cost money or can you put an interim solution to migrate them from one place to another? And your staff, are they trained on security? So all that are part in partial of the planning. So to remove those roadblock is to see ahead, plan ahead, eliminate as much as possible during that process. So when you hit the roadblock, its the last ten percent or five percent that you have to deal with instead of fifty percent while you rolling it out. That's the best I can give to anybody who want to implement this.

[00:08:41]
And when it comes to technology, as you know, in this day and age, technology is constantly changing. How would you overcome this when it comes to security and printing?

[00:08:52]
Well, adopt a new future. Right? Like I see it in terms of printing where it's become harder to secure. Before I was in an office, my staff come to work. I lock the room, they're inside this room. I don't really care. They print to printer, I put a gate maybe in front of it. Now I physically can scan people going in and out, but then the cloud comes in place. So my data center is no longer in very close to me. Maybe in the cloud, could be in US, could be in azure, could be in AWS. And so my data now, my data is travelling back and forth between the two data center and the office. My users are mobile. They have a mobile phone, they have the desktop, they have the laptop, they're moving around, they're traveling around. So they're mobile now. All those introduce a big factors to pick the right printer for them to print to, because of secure pull printing is an issue. The traffic that go back, leave my office that go to the cloud and come back is an issue. So what you have to do is keep watching for new technology because, you know, Azure is getting better every day, technology like, UniPrint out there to compensate the transition path from one to the other and adopting new technology so that your business can grow at the same time, still secure and comply.

[00:10:14]
Right. So I think the biggest point there. Would you say would be really just trying to future proof your technology, ensuring that technology is open to constant evolution?

[00:10:26]
Yeah. And there obvious some of the newer technology that you should try and look for, like make sure the solution that you put in would have two factor authentication, a piece of something that you own, something that you in your head. Make sure encryption is up to date. 1.0 versus 1.2. The encryption that keep being was very secure five years ago may not be anymore. The last two months

someone have managed to crack it somehow. Audit trail and tracking is important because sometimes you just can't protect everything. But you might be able to go back and find out where the hole is. Someone printed a whole part of visa card and walk away. It's very hard to track that live. But maybe after you can at least track back and say, you know what, Arron Fu was printed this, and this day and this is the list that he had. Hey, maybe it's not Arron, but maybe throw in the garbage and then that get tracked. So audit trail become important, as I say, secure pull printing is by far the best way to make sure that the user are picking up the right print jobs and the print jobs are not printed on the printer for someone to pick up.

[00:11:42]
Right. So for someone who may be new to the podcast, could you go further into detail on what secure pull printing is and how it works?

[00:11:52]
Yeah. There's multiple implementation of secure pull printing, I'll speak in terms of what we think is the best way, the way that UniPrint implement that every person have his own personal queue. So when you print from your mobile device, from your chromebook, from your Android device, from the desktop, from wherever or email to print, any which way that you generate print job, it gets into your personal queue. And in fact, the way that technology UniPrint work is, it turns into a PDF file and save it in your virtual queue. So you have a queue of all the print jobs. It's ready to print, but it's not released to anything yet. The beauty of that is the PDF being in an independent standard format. You can now take a print job and release it anywhere. So you can print anywhere. And when you do want to release, you are authenticated against your smart card, PIN, your AD directory, depends on how secure you want to turn it on. And then when you release a job, you are guaranteed to be in front of the printer either through your mobile phone or through a security device or an embedded application that's running on that printer. So in a gist is when you print, you don't get the print job until you are authenticated in front of the printer. So that's what secure pull printing is.

[00:13:13]
So would you say when it comes to creating a comprehensive I.T. security program for printing, the main physical and digital aspects you want to focus on is having a secure pull printing system in place that has two factor authentication as well as encryption and auditing.

[00:13:31]
Yeah. So you look at it from from the process of printing. So first you are authenticated when you do a print job. Right, so you need to secure that. When you print the print job, have to travel through wire. So encryption is important. So you got to make sure all the job that while during transit is all encrypted. The job when it is staged a secure pull printing environment, that job should also be encrypted so that nobody can peek into a hard drive and see what your job looked like. And then when you come to the releasing part, you need to authenticate the guy. So to prove that he's in front of the printer so that when that physical print job comes out, it will be the right person. And then there's the spooling of the print job right from your storage that have VQP in, to the point where the printer is. You can minimize because some old printer support an encrypted protocol. So what can you do about that? You might be able to put a device in front of the printer to make sure everything is encrypted and then have that device send a print job directly to the printer. Point two point, so that you don't have anybody can sniff the packet, for instance, pick up the print job. And so you're right. To summarize, you can say anything that goes on the wire needs to be encrypted. Anything got stored, what you call at rest, have to be encrypted and authentication should be at least two factor, maybe even three. Sometimes use your mobile phone, your pin and the user I.D. and then constantly enhance that encryption protocol and review the physical security, too. Right.

[00:15:12]
Right. And you did briefly mention auditing and tracking. Can you explain to us what is audit and tracking and why is it important?

[00:15:20]
Yeah. Thank you for reminding me that. Yeah, an audit and tracking is obviously kind of the end game for audit, for auditing right? Because if you miss and you kind of block and you can't stop people from getting that job, then one of the one of the thing that you can't prevent and most of the security breach come from the user, either they misuse or they are literally the one that actually leak the information out. But how do I track that guy, how do I find out how that leak is out? You rely on auditing, which mean I track every single print job, that being print on the network through our system. We even can make a hard copy of it or a digital copy of it so that I can see what the people are printing. And then I can track. So then when something do went wrong, I could go back two years from now and say, you know what, that list of visa number was printed by certain people in the office. Now, maybe I can track to him. Maybe he's the one who leak it or maybe he throw it in the garbage can, like I said, and then someone picks up and use it. So, yeah, auditing and tracking is very important part of the equation.

[00:16:34]
And now as companies are moving more and more towards the cloud, can you go over the importance of cloud security and how it might be different from on-prem security?

[00:16:44]
Yeah. I mentioned before that when they moved there how data now tends to travel up to the cloud and back down to the office. So under that circumstances, normally you put something called VPN in place to give you a virtual private network between your office and the cloud. But the reason why we have clouds sometimes is to support mobile user or home user. Right? So VPN is an expensive, hard to implement solution. So when you have a workstation at home, or have a mobile phone, the VPN sometimes doesn't work well. So under those circumstances you rely on the application on printing like UniPrint to encrypt by nature, all the traffic that's touched the wire. So it becomes important. Before it wasn't that important when you were inside your own office. So you know, nobody gonna be able to get into your office and tap the wire. But once you are in the cloud, everybody able to see your traffic in

that sense, it's going to pass through an ISV and gonna pass through an Internet provider. It's gonna be in the Internet and someone could potentially just pick it off the wire and you have to make sure everything is encrypted well before it travels through that Internet connection.

[00:18:01]
Circling back to the topic of compliance when it comes to heavily regulated markets like health care or finance. How would you go about meeting certain compliance requirements such as HIPPA or GDPR?

[00:18:17]
Lets see, HIPPA is not, sorry GDPR is not as important if you're not going to the cloud, right? Because if you own the data, it's your data center, you own the data, therefore you don't have to worry about. But when you use the cloud, then GDPR become important because the user have the right to that data. And that is the key. And is a policy driven thing. Right, so if I have an email address and I want it back, I need the data to erase from that service provider. So those are all compliance's that GDPR looking for, is that if I want to remove myself from Facebook, I need you to remove everything about me from Facebook. So I have the right to all those. And that is what its for. So its really for the cloud service provider to make sure that it's how that is done correctly. And as a company, you want it, you want your cloud service provider to that capability and compliance.

[00:19:14]
HIPPA is for health care. So in healthcare obviously, patient information is very important and all that all of that becoming an issue, if you are not HIPPA compliance, then I think Obamacare have a, I can't remember exactly when they are going to have that, HIPPA compliance, if you're not complying the several level, there's time, then then you'll be in trouble and printing is one of them. Right. Make sure you don't print your job and people will be able to pick up the patient information and stuff like that. And audit trail is part of HIPPA. Hope that answers your question. But I'm not a HIPPA expert in medicine. You gotta really, there's a big, huge document, obviously on the web you can go through it, HIPPA compliance for anybody.

[00:19:56]
Right. So after the show, we will link the show notes, and the show notes will link more information on HIPPA and GDPR compliance if you guys are interested in learning more on that. So just to to kind of wrap things or summarize things, what would you say is the importance of security and compliance and how does it enable businesses to function moving forward in the future?

[00:20:19]
I say it is a must for somebody who can afford it, in that sense. Small business don't really care that much because there's nobody going to go and microscope you. But as your business grow, it's very important to make sure your network is built on a secure platform. And so that you can grow your business. Right. So, as in this world, because as I mentioned, it is very on early on the show. Everything is digitized. So if you can't protect that asset, it's like I have a bank. I have a safe. I put all my money in there now, but then I didn't close the door properly. You need to close the door properly, put the lock in and do that. And this is a practice and require a lot of planning and put yourself on a good platform. And not only that, you have to constantly update this digital world are forever changing. So if you are in business, especially in the IT area, everybody is somehow in the IT nowadays, because I don't know whether, you know, nowadays the most expensive company in the world are all high tech company. So that is the area of growth, right. So you want to be in that business, you better be compliance. You better put your security. That's one of your top priority.

[00:21:36]
Awesome. So that's it for this episode of Printing Over Coffee if you are interested in learning more about print security and compliance. We'll be dropping a link in the show notes to our secure by design white paper, which goes into technical details of UniPrint's multi-layer approach to security. You'll also find links to this episode's transcripts as well as MP3 file for download. To get access to that, just head over to UniPrint.net/episode3. Thanks again for joining us and we will see you in the next episode. Bye bye.

END OF TRANSCRIPT