Real-World Security for Business Leaders
Transcript

Part 1: Top Challenges and the Evolving Security Landscape

Bill Pollak: Welcome to CERT's podcast series: Security for Business Leaders.

The CERT Program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at our podcast website.

My name is Bill Pollak, and I'm the manager of communications for the Software Engineering Institute. Today I'm pleased to introduce Pam Fusco, former chief information security officer for Citigroup and currently the executive director for security solutions at FishNet Security. Today we'll be discussing the challenges and opportunities for chief information security officers in the financial services sector, and how to build a viable information security program. So, welcome, Pam.

Pam Fusco: Well, thank you, Bill, it's a pleasure to be here.

Bill Pollak: Thanks for being here with us. So let's begin by just talking about: what are the two to three most challenging security and privacy issues for organizations in the financial services sector today?

Pam Fusco: Well, there's probably about 300 challenging issues, but if I had to categorize them specifically into a cluster, if you will, I think one of the top issues is staying abreast of the regulatory requirements when it comes to PII [personally identifiable information], as well as other regulatory issues. So understanding what's out there that we need to abide by, and then applying that inside of a corporation. And by that I mean understanding the regulation, interpretation of the regulation, and then implementation of it, which would be technology, process, procedure, policy, and governance. So that's one to two different things.

Bill Pollak: And it's the chief information security officer's role to stay abreast of those things?

Pam Fusco: Absolutely. And also abide by the policy, as well as manage the oversight of it. And by that I mean to measure to ensure that the policies that are put in place are accurate and valid, and also to take snippets. Perhaps it's scorecarding, doing some type of a sampling, analysis, evaluation, and collecting reports to make sure that we're abiding by the policies and meeting regulatory requirements. So it's oversight and governance. And in some instances, depending on the role of the security executive, it could also be the implementation of the technology pieces.

Bill Pollak: And is the regulatory picture constantly changing or frequently changing?

Pam Fusco: It changes quickly, absolutely. I think as, you know, we write laws because stuff happens. The same issue applies with regulatory requirements. But what we're seeing here is states pushing the requirement, and then the next one picking up, and the next one picking up, so we've really gained a lot of momentum with CA 1386, which is the California privacy law. It's now spread to, I believe, 39 different U.S. states, quickly to go to the full gamut, if you will. And then it will become a federal.

So that's normally what you would see down the pipeline. But we have several laws from a privacy perspective to abide by on any given day, on whether it's state, local, or federal, or international as well. So you're dealing with many different boundaries here, so it's difficult to keep on top of it.

Bill Pollak: Yeah, very complex.

Pam Fusco: Absolutely. But I think one of the most difficult pieces, though, is the interpretation. Some of these laws are guidelines, applied guidelines, so interpreting the guideline to reality across different business units can be a tedious task.

Bill Pollak: Anything else that you'd want to mention as a challenging security and privacy issue for organizations?

Pam Fusco: Communicating it. Why we do what we do, and so people understand what we're asking. I think that's really another issue that we need to keep on top of. Always, training and education is important.

Bill Pollak: Not just what you're asking also, but the motivation behind what you're asking, is that right?

Pam Fusco: Absolutely.

Bill Pollak: Okay, great. So, how do you determine which threats are most important to pay attention to, particularly given the increasingly targeted and stealthy nature of today's attacks, and how do you see the whole threat landscape changing in the next 12 to 24 months?

Pam Fusco: Every threat is important, but you certainly can't get to them all. So I kind of do a balance act. Those threats that have the greatest impact would be the ones that would get, of course, the most attention. And by that I mean, depending on what you have in your environment. So if there's an exploit out there that's indigenous to IE – Internet Explorer – you would definitely want to understand: (1) how much IE you have in your environment, and the majority of us have quite a bit; (2) the depth of the exploit or the threat, meaning does it grab an admin, does it overtake a system, does it have the potential to gain information from a system, or does it have the potential to get data from internal systems and services? So how deep does it go? So marrying all of that together kind of determines the level of attention you apply to a threat.

What we're seeing is a definite change in the landscape. And by that I mean we used to see a virus come in, kind of like the "I Love You" virus which came many years ago, and at that time we were like running around trying to ascertain, "Where did it come from, what to do, how do we get rid of it? " The reality of it was, if I look back at that now, it was kind of just minuscule on the map of where we are today. It was, you know, downloading a whole bunch of emails and inboxes and of course overloading inboxes and Exchange servers, but the reality of it was, it's a nuisance. Kind of like a DoS (denial of service) is a nuisance. It knocks you off the Net, but it doesn't grab information.

The landscape has changed significantly, by which [I mean] the fact that a virus comes in but also could dump a backdoor, a trojan, a logic bomb – very stealthy, very manipulative. So that's what we're seeing in the industry, a change there. What is difficult is the nature by which it's coming in. It's getting – it's very cloaked, it's difficult to check.

We certainly do try to keep up with the latest and greatest methodologies and technologies, but you know, if someone out there is producing an exploit, it's kind of like the reactive mode. We

don't know that it's an exploit until it's an actual exploit, so now we have to develop an antivirus signature, or a bug, or a fix to crack the situation. So at least trying to figure out what the next move is from a cyber attack perspective. And a big interest recently is the botnets, the bot herders that are out there, because you're talking worldwide, exploitable, perhaps zero-day, you know, minute-by-minute, download, exploit, just bringing everything to its knees. So keeping that in the forefront is very important.

Bill Pollak: And it sounds like what you're saying is that the organizational assets that are put at risk are more critical then they were, say, five years ago. Would you agree with that?

Pam Fusco: I think the assets have always been critical, but what I believe is that people understand security more. Understand what risk means more. That's driven by several variances: (1) it's widespread; (2) there's more out there than there was before; and (3) is of course regulatory requirements help that move along. We have to categorize your information: high, medium, low, or critical. So now we have a categorization, and we must protect. So I believe that it's prevalent and known that the information needs to be protected. Therefore, it makes it that much more valuable to an external party that wants to exploit it, if you will.

Part 2: Putting Security into Practice

Bill Pollak: I see, great. Okay, what have you found to be the most effective approaches for putting an information security program in place and ensuring that it remains viable? And what doesn't seem to work so well?

Pam Fusco: I think what has worked very well in the past is pulling together an internal consortium, sort of like a security advisory committee, panel, task force, working group, comprised of stakeholders within your organization or members of your business units that come to the table once a month, once a quarter, whatever works best for the corporation. I've seen great success. It gives people the opportunity to vet ideas. It gives them the opportunity to understand where you're driving security from. Is it IT? Is it business driven? And they also feel as if they have skin in the game, that they have a say-so. And it's widely accepted at that point, so it's not a surprise.

Also policy steering committees, whether it was a security policy or a corporate policy – bringing the right players to the table to understand what's coming. And then vetting that information to the populace, the whole corporation if you will, saying, "There's a new policy coming down the pipeline. Your input is just as important as everybody else's. You have three to four weeks to respond to any information, insight, recommendations you feel might be important to this policy." And it does a couple of things: (1) It gives the opportunity for insight; and (2) it presents awareness; and (3) we can say, "You knew this was coming. Don't give a blind eye to it." Plus, you have the opportunity to put input into it.

So, really, I believe communication and coordination and collaboration. It's not about the technology. It's about understanding and vetting that information. Where I've seen failure in the past is going out and commandeering a piece of technology or software and trying to force that down the pipeline. It just doesn't work.

Bill Pollak: So you have to build that buy-in internally.

Pam Fusco: Absolutely.

Bill Pollak: Great. Okay, what types of issues and opportunities do you bring to your senior executives and boards of directors, and what do you generally expect of them when you do that?

Pam Fusco: Issues and opportunities. I like to marry information security and risk management with business initiatives: (1) it sets a precedence; and (2) you have buy-in; and (3) it supports something futuristic, if you will. So what I like to bring to executive management and boards of directors past, present, and future – what we've done in the past, why it did or did not work. I bring failures to them as well, stating, "This was a project or a plan that was put in place, but it didn't succeed because of blah, but these are the lessons that we have learned." And I also bring what we need to do from a strategic perspective, and build in a piece of innovation.

I firmly believe that you can't continue to be successful unless you look into the future, kind of that crystal ball, and you ask business units where they're going in the next one, two, to three years, and marry that with your security strategy. So I like to bring to executives statistics: (1) what we've done and what we've done well, both from a policy-driven perspective, governance, operationally; (2) what we want to put in place that will drive the business out further, and why it drives the business further; and (3) time-to-market, how that enhances time-to-market.

And you know, it's difficult at times to get an ROI [return on investment] on security, but there certainly are advantageous solutions that we can put in place to prove an ROI. What comes to mind right now is identity management, getting a grip on that; standards and regulatories around policies, maybe marrying it to an ISO standard, if you will; across the board, processes, procedures, and system life cycle development; as well as document integrity, and bringing that to the regulators as well as executives. And then, "What's happened outside of us?" and saying, "This could be us, but because we have X, Y, and Z in place, it wasn't." Which kind of gets you to the next step, saying, "I've proved my worth. I want more. To contain and to protect and to respect the integrity that we have."

Bill Pollak: Sure, great answer, thank you. When you can't do everything that you'd like to do, how do you go about making the necessary trade-off decisions and prioritizing security investments, and what percentage of an organization's IT budget should be allocated for security?

Pam Fusco: You know, you'll never be able to do everything that you want to do. I think you just kind of have to come to grips with that. It takes a long time to realize that.

Bill Pollak: Well, you've given us some great strategies for building internal buy-in, that's for sure.

Pam Fusco: And that's all learned through pain, let me just tell you. You know, in my younger days in the information security profession, I thought that we could just do it all. And for various reasons, the business isn't going that way, the budget isn't there, you don't have the internal knowledge.

See, the trade-off is this: I believe that any plan that's built must have flex built into it, because if it does not, then it's not a good plan. If you build a three-year strategic plan, and you pull out the middle piece, does that mean the whole plan crumbles, or can you continue to move on? So I really like to build flexibility into a three-year strategic plan, or a two-year, even a one-year, if you will, but that's more of a tactical-driven solution. The trade-off would be understanding what I'm giving up and what the impact is. If I'm giving up adding additional firewalls, I already have some, I can make what I have work, that's fine. Is the trade-off not having a management console to manage all of my different security solutions, which I'm really looking forward to, to provide metrics and reporting and so on and so forth? That's going to be a harder pill to swallow. However, I would like to say, "I will trade this off if I can put phase one into place this year. And then do phase two and phase three the next year."

So really, if you can stagger it, I think you can, at the end of the day, get what you need to get. But you really have to stand your ground and show what you don't have and what you don't get, what the impact would be. And then again, there are trade-offs, and everyone across the board has to then accept the risk of what the outcome could be if you don't do what you said you were going to do.

Bill Pollak: So it sounds like you go in, part of your plan is knowing what your priority is for each of the elements of that plan. Is that right?

Pam Fusco: Absolutely. And set the expectations too.

Bill Pollak: And what are the sorts of things on which you would find it most difficult to compromise?

Pam Fusco: I think the most difficult: operations.

Bill Pollak: Operations, okay.

Pam Fusco: Giving up security operations. And by that I mean, I don't mean by outsourcing or whatever, but not dedicating enough to security operations. Incident response – we would be weak to think that because everything is running so smoothly and you haven't had an incident that impacted you at 2 AM in the morning for the last month, that you can lax. That is definitely not true. I would not give up on – you know, the thing that you normally do have concede on is training, unfortunately. But I really like to stand my ground on that from a training perspective, not just from my staff, but everyone involved. And then the other piece that I really won't give up on is compliance. And if I have to step back on that, that's fine. I try to look to a legal entity to kind of flip that bill for it or switch it over to a privacy person or a risk department, to say, "We can't fund it, but you need to." So maybe it's a trade-off. We give and take from different departments.

Part 3: Security as Business Enabler

Bill Pollak: Great. I think that will be a very helpful answer to our listeners, thank you. So what are the first steps that a business leader can take to develop an effective plan for information security?

Pam Fusco: I think that you need to ascertain the state of security that you're in. And for a business leader, I think from an information security risk management perspective, it's our responsibility to let them know what exists today. It's our responsibility to share with the business leaders what the future vision is and then obtain from them what their plan is, and help them foster the program that they need to put in place, because you're talking from a business perspective, correct?

Bill Pollak: Yes.

Pam Fusco: So to build on an information security program, they certainly do need to be behind it. From a regulatory perspective, it makes it that much simpler. I can't think of any business that is not regulated at this time: healthcare, finance, pharma (pharmaceutical), R&D (research & development), educational, online retail, everything is regulated. So, from a business perspective, time-to-market is very important, and if security and technology is a part of that, that's certainly going to help you get to market quicker.

There have been studies done within the pharmaceutical industry where one pharma went to market 30 days before the other on a similar drug, and the pharma that went to market first was

always ahead of the pharma that was behind for the next ten years. So, 30 days is a meager amount of time, but the reality of it is, from a business perspective, getting to market quicker. The reason pharma A got to market faster than pharma B is because they could plug and play with their subsidiaries faster, and it was the security.

Bill Pollak: Oh, it was?

Pam Fusco: You know, VPN (virtual private network) solutions, so on and so forth. Knowledge transfer, sharing of documents, data integrity, they just put it up quicker then the other pharma did. So, really, there's a real case study out there that says, you know, it's not just from a risk perspective, or getting hacked or compromised. It's a business perspective as well.

Bill Pollak: Interesting. You would think, just not knowing much about it, that security would be counter to time-to-market. But what you're actually saying is that...

Pam Fusco: We're trying to change that, okay?

Bill Pollak: Yeah, right.

Pam Fusco: I see security as totally evolving. It's not a bunch of geeks in a back room. Our hair isn't dyed pink anymore, although some might be. But the reality of it is, we're a true profession. And it's a young profession, but it's really now a true profession. We have certifications, accreditations. We have accountability. We have reliability and responsibility. And I think all of that together makes it a reality.

Bill Pollak: Also, I think, fully integrated into the operations and computer systems as opposed to something that's kind of tacked on.

Pam Fusco: Absolutely.

Bill Pollak: Yeah, great. Okay, so what are some special concerns that a chief information security officer must take into account when working with a large organization?

Pam Fusco: Everyone has an opinion.

Bill Pollak: That's not only true of large organizations.

Pam Fusco: Everyone's opinion should matter. You may be a part of a large organization, but that doesn't necessarily mean that you deploy largely. It's probably a task-driven, phased approach that you want to do a deployment in. And that you need to make sure that you have buy-in across the board, which probably is going to take the longest part of the whole. And you may not get 100% buy-in across the board. That's okay. As long as you have the majority, and it's understood why you're doing what you're doing, again then I believe that you'll be successful. And repeat throughout the process or the program that you're deploying, milestones, the success of, or again, if you have a setback, communicate why, and what you're going to do to correct it. So always keep them on top of it, because I've seen so many projects put into play that are funded for two or three years, that just up and die because people forget about them. So, you know, do all the pieces from a technology perspective, but keep communicating why you're doing this project so it's always in the forefront of folks' minds.

Bill Pollak: Well, thank you, this was great. Where can our listeners learn more about some of the things that you've talked about today?

Pam Fusco: There's many different facets. There's forums and consortiums. I work with the Carnegie Mellon lab here, CyLab. They're awesome. They do a great job. They have a lot of cutting-edge, R&D, forward-thinking programs in place. CERT of course is a real-time tactical, if you will. Many of the vendors have very fantastic sites that you can go to and get information, training. There's the CISSP (Certified Information Systems Security Professional). There's the ISSA (Information Systems Security Association).

I encourage security professionals to get involved in a external security consortium, so they can understand what's going on outside the confines of their organization and kind of look at what the competition's doing, or look to see if they're better or worse, or pick up best practices along the way. So get involved with your ISSA chapters as well.

Bill Pollak: Well, great. Well, thank you very much, Pam.

Pam Fusco: It's been a pleasure, thank you.