

## Concrete Steps for Implementing an Information Security Program Transcript

### Part 1: Leadership Roles and Aligning with Business Strategy

**Julia Allen:** 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](http://cert.org).

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

My name is Julia Allen. I'm a senior researcher at CERT, working on security governance and software assurance. Today I'm pleased to welcome Jennifer Bayuk, an information security specialist and former chief information security officer at Bear Stearns. Jennifer and I will be discussing the necessary steps to set up an effective, sustainable information security program, a tall order. So welcome Jennifer, glad to have you with us today.

**Jennifer Bayuk:** Thank you Julia, glad to be here.

**Julia Allen:** So in your experience, just to get us started, what roles in an organization are in the best position to initiate and champion a strong program?

**Jennifer Bayuk:** Any role with control over technology is going to be in a great position to champion an information security program, such as a CIO or a chief operating officer. In the absence of that, it's not likely that an information security program would be effective.

**Julia Allen:** So you mentioned the chief information officer or the chief operating officer. Are there some other roles that you've seen, senior leadership roles, that can kind of catalyze getting started?

**Jennifer Bayuk:** Well the CEO is always the best catalyst. The tone is set at the top. So just the idea that information protection or privacy is a value of the organization as a whole will have influence. So, for example, if there is a strong tone at the top that employee information is to be protected, then HR [Human Resources] could develop their own security awareness or information protection program and it would be generally followed.

**Julia Allen:** Occasionally I'll see in our governance work a chief risk officer, if the organization has one, or maybe even audit playing a role. Have you seen those roles kind of serve as champions?

**Jennifer Bayuk:** Those roles can serve as champions, yes, and they're often invaluable sources of expertise in program implementation. But because they don't control resources directly, without the tone at the top, they would be an ineffective champion. So they are great in conjunction with someone who controls and directly

influences technology and information flow, but by themselves they won't be able to pull it off — put it that way.

**Julia Allen:** Well that makes good sense. So while we're at the senior leadership level, what are some of the oversight or governance responsibilities that either an information security manager or a CISO should be playing, in your experience, particularly with respect to making sure the security program is aligned with the business?

**Jennifer Bayuk:** Business alignment always comes from the recognition of what information assets or what technology processes are key to enabling business objectives, to begin with. So the way to make sure that the program is aligned with the business is to understand how the business operates and what information it uses and what the data flow is through the systems that are used by the business to achieve its own objectives every day.

The risk management component is really key to motivating executives to even think about an information security program. Why would they have one at all if there weren't some kind of risk of having intellectual property in the hands of competitors or exposing their customer data to identity theft or some other types of risk that would put their own business with their own customers at risk?

And so as you are looking at how to develop a policy or a strategy around a business objective, you need to be thinking about that risk in the same way that the business leaders think about it.

So if the CISO or the information security program manager understands that or has an ally on the business side that will help them identify those information assets and the data flow, then they will be able to devise policy awareness and implementation around those business objectives. It really does start with a business strategy and then the information technology that supports that strategy.

## **Part 2: Building on Strategy, the Five Key Components of an IS Program**

**Jennifer Bayuk:** So once you have that strategy in place, the second component you need is some kind of policy, which is a documented, agreed upon set of mandates that the authorized individual, the tone at the top, believes will accomplish their goals for information security.

Of course, once you have the policy, the policy is a document sitting on the shelf unless everybody reads it. So you need to have some awareness activity, which is an important component of any information security program. Within awareness activity I considered training activity and all the types of outreach you need to do to make sure that those with roles and responsibility for security actually know what they need to do in order to accomplish the goals for security, as dictated by the policy.

**Julia Allen:** Have you found in the awareness realm some particularly effective ways? We hear about standard training and education and perhaps certifications and things

like that, but in the organizations that you've worked with, have you found some kind of unique or innovative approaches to keeping awareness high in the organization?

**Jennifer Bayuk:** One key awareness message that I think is included in all of the best awareness programs is that security is everybody's job function. It is not the security people coming here to train you. It is that your job includes a security component and this is what it is. And the level at which the security program can bring that message home and provide the awareness, training, education and tools that each person with a role, that includes security, needs to accomplish that objective of that role – that's the extent to which it will be successful.

**Julia Allen:** So have you seen some efforts on role-based awareness and training where you target a particular outreach initiative to, say, system administrators or application users of a particular type of process? Do you see that working?

**Jennifer Bayuk:** Yes, definitely. You do need to have the training be aligned with the job function and let people know what is it about their unique situation in the organization that makes it so appropriate that they embrace security as part of their role.

Special training for the Help Desk is very important. How do you service someone and still protect the information that someone may be asking for? You need to give these people special tools and techniques to deal with their special situation, and it applies across the board to every unique situation.

System administrators that you mentioned is also a very special case. How do you keep the system up and running and allow people to access the operating system facilities that they need to do their job without giving away the keys to the kingdom? Where is the line that you draw between your responsibility to protect the information and the operating system facilities versus your responsibility to provide access? Right? So if the security program can make it very, very clear where that line is drawn, then the system administrator is not only trained but empowered to execute that responsibility in a way that they know is endorsed by upper management. And that tone at the top that authorizes the security program. It really does empower them and it really sends home the notion that security is part of my job function.

**Julia Allen:** Okay, so you've mentioned strategy, policy, and awareness as the first three of the six components you recommend. Could you tell us about the other three?

**Jennifer Bayuk:** Yes, well once you have awareness then implementation should follow. If everyone knows what they need to do for security then you get implementation that is aligned with strategy. However, even the best intentions and the best trained people sometimes fails for unforeseen reasons, and so in addition to the implementation program component you need a monitoring component. And the monitoring component needs to look at implementation with strategy and policy as compliance as its objective.

I think monitoring is very important because monitoring should always look directly at implementation and do some kind of comparison – as automated as possible but in some cases it can't be – but as automated as possible to validate that implementation is in line with policy and in line with management objectives.

**Julia Allen:** So during monitoring, is that where you might do some self-assessment, for example?

**Jennifer Bayuk:** Self-assessment is one type of monitoring. However, self-assessment is also a very important component of awareness because in your training and in your pre-implementation phase of implementing policy, an assessment is an important tool that brings awareness of implementation strategy that will be effective and brings that into the implementation.

So when I speak of monitoring, I'm more – I'm not really talking about pre-life cycle or pre-deployment improvement efforts but of real-time monitoring of actual configuration. And audit is part of that, and you can consider audit as a special case of self-assessment, especially internal audit. So they're not entirely completely different – monitoring and assessment – but when I speak of monitoring as a component of the program, it's really this feedback loop to make sure that what you already thought, based on your analysis, education, and training should be implemented, actually does reflect policy.

I think there's a common confusion between "Did we follow the right process in getting something implemented?" versus "Is it actually implemented according to management objectives?" And monitoring components are the latter. They are sanity check, right? Is it right?

**Julia Allen:** But I mean sometimes in the measurement arena, you hear a lot of conversation about process metrics versus outcome metrics — where, as you said, validating that the process has been adequately followed but may or may not be producing the right outcome. So do I hear you correctly in that during the monitoring phase, when you go back to business objectives, you're really trying to make sure you're doing the right thing?

**Jennifer Bayuk:** Definitely, definitely. Monitoring process does help as well because once you have found that you're not doing the right thing, then you need to correct it. And you go into the last component of the information security program, the remediation component.

When you're in the remediation component, you need as much information as possible. So if you've been monitoring the processes you can tell where the process, even though it was followed correctly, had an inaccurate result. And you can change the process and change the things you monitor about the process, and hopefully more closely align the process with the desired result.

So in the remediation activity, you get feedback from the monitoring process on all of the awareness, implementation, policy, and strategy processes. It could be in the

remediation process that your recommendation is not for some change in a procedure or a technical security measure but for a complete change in organizational structure because the process that you put in place didn't turn out to have the right authority, the right management buy in, or the right business alignment. So the remediation activity will feed back into the strategy, and that completes the loop that gives you the continuous feedback for the security program.

### **Part 3: Measurement and Automation**

**Julia Allen:** I would expect that through all six components or activities you need some way of measuring how you're doing. We talked about it a little bit in monitoring. But in your experience what are some of the important measures you've used to track and report the status of the program?

**Jennifer Bayuk:** You'll need to use different measurement strategies for different objectives. But I can break them down into basic categories of measurement. You have measures that are target measurements – for example, that you are implementing something and you are trying to make sure that you are getting 100% coverage; say an identity management system. You want every user and every operating system and application to be aligned with an index number in your identity management system and that will be a target of 100%.

So one type of metric that's important is to know what your entire universe is and then know how far away you are from that target in an implementation. And then you have a monitoring metric which goes a little bit more into the process where you might be looking at technical measures but you're also measuring the remediation process or even the implementation process where you've defined a process that you believe should have the result of getting 100% to your target metric, and it contains decision points that have to be executed by individuals to ensure that the target will be met.

And I'll give you an example of a configuration metric that has a process behind it that is designed to keep the implementation of the configuration correct, in something I think most people understand like a firewall rule set.

So you have a firewall rule set and you want it to be correct but it changes all the time. So you can't just say "This is the correct configuration, yes or no" like a target. So you have to say "What is the process by which the firewall rules change and how do I know that that change is accurate?" And to do that you need to create a process for change control authorization and know that as people execute that process they are making correct decisions. So you need a monitoring metric, not only to show that all of the firewall configurations are monitored, that changes are automatically detected, that they are reported, but when those changes are identified that there is some validation that they were authorized by someone who can actually look at an authorization process and a change management plan and see that that change that occurred technically in the firewall does match what was authorized.

That's a decision point. How do you know that decision point was made correctly? Only by monitoring it. So you're actually putting a layer of monitoring, management monitoring, over the actual execution of the process that is meant to give you a target metric.

**Julia Allen:** Right, and then from that I would conclude or infer that that then – if you have those processes in place, the monitoring processes, the decision points, then clearly that gives you confidence that your security program and the controls that you've put in place are operating as intended.

**Jennifer Bayuk:** Yes, it gives you confidence, and then in addition you'll still want to do, as you pointed out earlier, the assessment, the audit, the overall sanity check that the confidence is deserved.

**Julia Allen:** So given all that – I mean, that's a whole lot of activity and processes, metrics, outcomes, decision points, to put into place. And I've heard you speak to the essential need for automation of security controls. So could you say a little bit about where you've seen automation work particularly well and perhaps where not?

**Jennifer Bayuk:** I believe that automation does work particularly well in areas that are more black and white, like target metrics and change detection and anything that you can pre-determine in advance exactly what a positive or a correct outcome looks like. I have seen automation in areas of security management and process that are less effective when they are instead concentrating on the decision points or the human oversight part of a security program.

I can give you an example, say, in vendor management where you have requirements for vendors to secure data. And there is a lot of checklist-type requirements that people have – the vendors must have a security policy; the vendors must have a secure file transfer system; the vendors must have a way to encrypt email; checklists that you would have for a service provider that is handling information that you would like to see adequately protected.

So you have your requirements and you need to now apply those requirements to the vendor environment. That is a place where automation doesn't help. Every vendor is different. Yet there have been attempts to automate that by allowing vendors, say, to go fill out surveys or checklists or spreadsheets and then taking those results and deciding how risky it is to leave your data at a vendor site, based on some automation on those results, which are already abstracted from the vendor environment because the vendor has control over the decision points that give you the measurement.

The automation part there is not as effective as if you had just stepped back and said "Maybe we can't automate the initial part of the review. Maybe we really need to look at this manually first before we start playing with the results."

**Julia Allen:** Right. Like anything else, you've got to – as you said, it's got to be black and white, well defined, quantitative versus qualitative perhaps, before you can –

you need to understand the manual steps well and they need to be rigorous before you can say "Okay, let's automate that part of the process," right?

**Jennifer Bayuk:** Correct.

**Julia Allen:** Well Jennifer this has been a fantastic introduction to a very, very difficult and complex subject, and I appreciate you breaking it down for our listeners. Do you have some sources where our listeners can learn more?

**Jennifer Bayuk:** The book that I wrote on *Stepping Through the InfoSec Program*, that's a good source. The ISACA COBIT model and the ITGI governance model that they have been publishing and continuing to work on are also very good sources of information on how to accomplish some of these objectives for a security program. In addition, there has been a lot of interest in I-T-I-L, the IT Information [Infrastructure] Library, as a possible source of integration with security programs, and there's a lot of good ideas about service and service delivery with respect to security there as well.

**Julia Allen:** Well Jennifer, I very much appreciate your time and your expertise today and sharing what you've observed and learned throughout your career with our listeners. I've really enjoyed our conversation, so thank you very much.

**Jennifer Bayuk:** Thank you Julia.