Connecting the Dots between IT Operations and Security
Transcript

Part 1: The Disconnects, and Why Business Leaders Should Care

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.

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 executive outreach. Today I'm pleased to welcome back Gene Kim, Chief Technology Officer for Tripwire, and a founder of the IT Process Institute. Gene's first podcast on the critical role of change management provides the foundation for today's conversation. We'll be discussing effective ways to connect the dots between IT operations and security professionals. So welcome back, Gene.

Gene Kim: I'm glad to be back, Julia.

Julia Allen: So just briefly, to bring our listeners up to date, when we last spoke in November of 2006, you had just published the IT Controls Performance Study. The study identifies the foundational controls that have the greatest impact on IT operations, security, and audit performance. And now, with your co-authors, you've recently published Visible Ops Security, with the subtitle Achieving Common Security and IT Operations Objectives in Four Practical Steps. No mean feat.

So just to start us off, based on your interactions with clients and customers, what have you found as to why IT operations and security staff are so often at odds with each other? And why do you think business leaders really need to pay attention to this disconnect?

Gene Kim: Yeah, Julia, it's funny. I think you and I have both had a common passion of trying to understand how does information security operate in the context of the entire organization? And I think over the years, the dysfunction that we've observed, we can actually diagnose pretty quickly. I think it's got two areas of dysfunction. One is when operations, or rather, specifically IT operations, will make life difficult for information security by, for instance, deploying an insecure component into production. In other words, maybe information security standards were never written down, let alone implemented. Perhaps due to the time-to-market pressures, corners were cut that forced it into production before those security features could be enabled or built.

One of the things that also makes life difficult for information security is that IT operations often has many, many things under management, but has never been documented or is written down in one place. And so this makes the production landscape of all the IT infrastructure under management very, very difficult to understand. And if you can't find it, you certainly can't manage it.

Julia Allen: Well sure. And I mean, the operations staff are under pressure to make things work and keep things running. And I would imagine that security is sometimes – if it's on their radar screen at all – it's an afterthought.

Gene Kim: Oh, absolutely. And I think to make life even more difficult for IT operations is that they're often very challenged to deliver against the availability objectives that they have. And what

that causes for information security is that IT operations becomes even further behind in their own work, and so therefore the information security work gets back-burnered.

Julia Allen: So why should this gain more attention of business leaders? How does this end up showing up at the business level, this disconnect?

Gene Kim: I think there's a couple reasons. One is that when these things happen, when operations can't achieve its own goals, then it certainly can't achieve security goals. Or when it does, it does it under tremendous time pressure, and often does not the best job that it could have done.

I think a second thing is that information security makes life often more difficult for operations by maybe unintended creation of controls that create additional bureaucracy, which actually increases the backlog of reviews. Security gets in the way of being the last step in the review cycle and it can actually hold up critical IT operations projects.

So the reason why the business leaders need to care is that not only are these two organizations, IT operations and information security, getting in each others' way, but neither are achieving their objectives. In other words, IT operations isn't providing a reliable, stable, and secure IT production environment. And information security is certainly not achieving the goal of safeguarding the business goals and objectives, whether it's things on security breaches or compliance with laws and regulations, or the identification and creation of controls that actually can reduce business risk.

Julia Allen: Well that makes good sense, so that's a great segue into my next question, which is how do we get security to focus on what is most important to the business, and hopefully then get business leaders to care more about security?

Gene Kim: Yeah, that's a great question. I think about what we found in the research that we did for Security Visible Ops was becoming more specific about how to sort of get below the platitudes. In other words, the statement of "buy low, sell high." Well, that's certainly correct, but it's certainly not actionable. So the first thing we did is become more specific about what those information security objectives really are. One is certainly the desire to quickly find and correct for our security breaches, ideally before anyone is impacted, especially customers. There's this custodial relationship to prevent the loss of confidential or personally identifiable information. Security, also by helping create stable and secure infrastructure, helps provide reliable IT services – and especially when the business depends upon them for business operations. That's absolutely critical. And perhaps the most visible for business leaders is the need to be in compliance with laws and regulations. For example, the Payment Card Industry standards, the HIPAA, SOX-404 – the compliance du jour problem, all of which jeopardizes, puts the organization at risk of being on the front page news.

Julia Allen: Well, I know that compliance has been a big driver for raising the profile of security in organizations. But I think sometimes we have the tail wagging the dog, because you really want to make sure that your compliance requirements make good business sense, and ultimately, one of my thoughts is, security can really serve as a huge enabler for other types of business relationships – perhaps global supply chain partnerships, things like that. What do you think?

Gene Kim: Well, absolutely. And I think what became very evident to us is that I think we started to realize what information security looks like when it is meaningfully providing value to the organization. But we became even more interested when we sort of wrote down how information security is perceived when it isn't doing that. And these are the words we wrote down that I think some of us in information security have been labeled over the years – words like "crazy, hysterical,

irrelevant, bureaucratic, bottleneck, difficult to understand, not aligned with business needs, shrill, perpetually focused on irrelevant technical minutia."

So I think it was, on one hand, sort of a tough thing to write these words down and admit that "yeah, some of these words have been associated with information security." But also to say that "Hey, there are things that high performing IT, information security organizations, there are things that they do that actually genuinely add value, which are really the opposite of the adjectives I just listed.

Part 2: Benchmarking and Situational Awareness

Julia Allen: Well sure. So to begin to turn that perception and reality around, Visible Ops Security, at least based on my reading, describes a set of proven sound practices that IT operations and security teams can use to operate and maintain production systems, as you said, meet compliance requirements and provide for new business-driven services.

So I think it'd be kind of interesting to explore a bit how you went about selecting the actual practices that you chose to include in the guide.

Gene Kim: What we found was that there were certain characteristics that all of these information security organizations had, and that was this notion of business aligned, plugged in into the production environment and plugged into the other processes where the work is being done. Because information security doesn't do all this work, it has to integrate into the work of others. We found that they were adding value.

So each one these stakeholders, such as IT operations, the software development and application development processes, release management and project management, all saw information security as a critical stakeholder, to the extent where these people would, when they'd conduct meetings, if security doesn't show up then they'd actually wait for security and reschedule if necessary, which I think is a great indicator that security's really adding value. That these information security organizations were able to scope and prioritize in a very specific type of way. And were also people savvy – that they were always interested in how they could add value to the other parts of the organization and help them achieve their objectives. And of course then, simultaneously achieve their own information security objectives.

Julia Allen: Well, and from your IT benchmarking work, clearly you're starting to see this kind of behavior in a wide range of organizations, correct? Not just specific sectors.

Gene Kim: No, absolutely. This seems to span all different company sizes as well as all different industries. And I think what was especially interesting is that it wasn't what's good for one set of compliance regulations is good for virtually all the other compliance regulations. It was all about how do you maintain and help the organization maintain a certain set of rigor and discipline.

Julia Allen: Boy, that sounds very solid, foundational, and very promising for organizations that are struggling with these issues. So let's turn our attention to understanding a little bit more about what you recommend in Visible Ops Security by briefly walking through the four phases. As I read, you call phase one "stabilize the patient and get plugged into production." So what's involved in phase one, and particularly, why do these activities need to be done first?

Gene Kim: For us, it was a very important phase. And I think the key term that we used in this chapter, and actually throughout the entire book, was the notion of situational awareness. So the goal of phase one is really to get plugged into production and gain a level of situational awareness

where security is not the last person to know that something big is going to happen, and it finds out only after it, say, gets deployed into production, blows up and causes a security breach. So what we want to do is, from an informal perspective, go beyond finding out at the last minute and gaining a level of understanding of how the organization operates, who the critical stakeholders are, what the major projects are. And we can do this from an informal level.

But ultimately, what we want to do is get actually plugged in to the IT operational processes where the work is actually done. So there are three areas that we want to get plugged into. (1) The first is integrating into change management. I think change management and security are in some ways kindred spirits. They're both actually chartered with the management of risk. And there's many things that information security can do to add value to the change management process. One is by helping manage by fact and insuring that all changes are authorized and actually going through the change management process. And this creates a way for information security to help create a culture of change management. Information security can also help by really creating tone at the top. By making sure that IT management takes decisive action when people make unauthorized changes. And in this age of compliance, when the organization does these things well, information security can make it very easy to substantiate the effectiveness of controls for audit and compliance activities.

Julia Allen: So when you talk about situational awareness, you're really talking about security getting a very accurate handle on the production environment, what's coming into production, what some of the projects are that are in the pipeline, clearly understanding the threat and risk landscape, and just having a good picture of the lay of the land, so to speak. Right?

Gene Kim: Absolutely. I mean, what better place to find out what out the organization is working on and what they have scheduled by looking at the release calendar and the schedule of upcoming changes. So it's actually a very powerful place for security to gain visibility of what the organization is working on. Absolutely.

And there's two other areas that are in scope for the first phase of Security Visible Ops, which is (2) plugging into the access management processes. Insuring that IT management is – that all privileged accounts can be traced back to a real person and an authorized approval from an authorized manager.

(3) And then the second area is integrating the security incident response procedures into the IT incident management processes so that security can – if they can codify up front what constitutes a real security incident, integrate that so that security doesn't have to create a whole 24/7 help desk function.

Julia Allen: Yeah, I do find this common theme, which is the notion of taking well defined security controls, in this case incident response, and integrating it into mainstream operational processes as one way to get effective change going on in the organization, and allow it to be a sustainable capability, right?

Gene Kim: Absolutely. And I think, well, we're able to say with a great deal of specificity, "Here are the specific activities and in the order you should tackle them."

Part 3: Risk-based Scoping, Upstream Involvement, and Meaningful Metrics

Julia Allen: Okay, so for phase two, which you call "find business risks and fix fragile artifacts," I'm curious in exploring a little bit the steps that you recommend there and in particular why a risk perspective is so crucial.

Gene Kim: I think for us the SOX-404 lessons made evident a very interesting cautionary tale. When the SOX legislation was first passed, in year one of SOX, one of the things that was very evident was that it was generating a tremendous amount of work for IT management, but it was also generating a lot of findings. So if that weren't bad enough, we also then found that upon analysis, most organizations, when it looked at these IT findings, could actually throw them out because you could say with some degree of certainty that those findings couldn't result in an undetected material error that would result in inaccurate financial statements. So the uncomfortable question that you could ask is, "Well then, why did you test it in the first place?" And the answer is that "Well, you shouldn't have." In other words, it was actually a scoping error.

So Julia, you and I worked on the GAIT project with the Institute of Internal Auditors to really codify how to appropriately scope the IT portions of SOX. And GAIT has now been extended to go beyond just the internal control objectives for financial reporting, but also complies with laws and regulations and IT operations. So it's all based on risk.

So the goal of the phase two of finding business risks and fixing fragile artifacts is to really use the GAIT principles to scope appropriately where do we have reliance on critical IT functionalities, and be able to say that with black and white terms – in scope or out of scope, and use that to scope our IT work.

Julia Allen: So obviously, you know we can't secure everything, we can't implement every security control, it doesn't make good business sense. So based on the GAIT work and other experiences that you've had, this whole notion of using risk kind of as a knob or a handle to help you rank, stack, and prioritize which controls to implement based on their criticality to the business, that's really the message, right?

Gene Kim: Absolutely. I think this provides the tools for us to focus on the few that matter. And often, it isn't a few, it is very many. But fewer than it would have been had you prioritized everything the same. And one of the things that phase two will require is an end-to-end view of the business process. And often, this actually requires a tremendous amount of work. But luckily, there are people in the organization that probably have done this work already. Probably most specifically business analysts or internal audit. So here's a way that we can actually reach out to them and help them achieve their objectives by making sure that we are on the same page in identifying where does critical IT functionality reside? And what steps must IT take to insure that those controls are effective and working?

Julia Allen: And what is a fragile artifact?

Gene Kim: A fragile artifact was a term that we used in the first Visible Ops that was really targeted at IT operations staff. Fragile artifacts are those fragile pieces of infrastructure that are prone to break, have high business outage costs, have high meantime to repair. So in that context, fragile meant operationally fragile. In this book, we extended that concept to have fragile not only mean operationally fragile but also fragile for laws and compliance with regulations or internal control objectives around financial reporting.

Julia Allen: So again, you used the concept of fragile artifact to help prioritize where security and IT operations should be paying attention.

Gene Kim: Absolutely. And by the way, I think another way to reword fragile is "risky." Where does risk reside in the IT infrastructure?

Julia Allen: I think that's a really important concept for helping determine where to focus attention. So let's move on to phase 3, "implement development and release controls." Could you summarize these for our listeners? And in particular, perhaps call out why it's important for security to integrate with other organizational functions like internal audit, project management, and the software development life cycle.

Gene Kim: The goal of this phase is really to integrate into the upstream processes so that we can build quality and security into the software products and services. So this means working together with those organizations that are actually developing those applications – includes working with the project management function; even to some degree the finance controls to help insure that controls in and around project management are working; and even internal audit.

I think for application development that the key activities include helping codify security standards, training the development staff to use secure coding practices, creating a library of reusable code that security has pre-approved. And it saves them time and enables them to have better outcomes when they actually deploy into production so that the applications and services aren't fragile and insecure.

We also will integrate into the QA (quality assurance) functions. And you talked about sort of an affinity, there's a natural affinity between information security and QA. We can help them. In fact, they can also help us by testing, as part of their protocols, information security risks.

Julia Allen: And what about internal audit? I know you spent a lot of time researching and codifying the relationship between security and internal audit.

Gene Kim: I think internal audit is sometimes a sensitive topic, because internal audits will strive to maintain its independence. But what we found was that information security should have an informal relationship outside of the annual audit cycle, primarily to make sure that we have a common view of where the highest organizational risks are. And as information security shows that it can do a great job, information security becomes a very valuable part of the IT management team and becomes a great liaising function for internal audit. So when it does its job well, we can help the organization spend less time prepping for audits. We have fewer audit findings, maybe more importantly, fewer repeat audit findings, and less time fixing issues. And of course, those are all by-products of having the organization managing risks well and achieving its goals and objectives.

Julia Allen: So moving to the last phase that you call "continual improvement," this seems to go with every process improvement activity that we as a community tend to define. So what's unique about the continual improvement phase in Visible Ops Security?

Gene Kim: Julia, I think you're absolutely right, continual improvement is certainly not unique to Security Visible Ops. What we tried to do is really codify which outcome measures are the most important, and which metrics are the ones that matter, as demonstrated by the nearly 1,000 IT organizations that we benchmarked.

And so each one of these metrics and outcomes that we're looking at are specifically tied to the activities that we describe in each one of the three phases. And we describe short-term metrics outcomes and we also described longer-term metrics and outcomes.

Julia Allen: So could you give us an example of some of your favorites?

Gene Kim: I think I have two categories of favorites. I think from the security perspective, my favorites are: what percentage of security breaches result in some sort of loss event? Is it reputational, financial, and so forth? All organizations, even high performing ones, have security breaches. But high performers have a far higher probability of fixing it quickly enough before it turns into something catastrophic. Another metric is: what percent of security breaches are detected by an automated control? Again, high performers have controls built into daily operations, so that they're found internally in an automated way, usually measured in minutes, as opposed to weeks or months, with far less impact to the organization.

I think two other metrics are around compliance, which I think will resonate with many people who are having to comply with these regulations, which is: what percentage of the organization's time is spent prepping and liaising with auditors? And how many repeat audit findings are coming out of those?

I think from an operations perspective, and people who are familiar with the first Visible Ops work, this will be very familiar: what percentage of the IT organization's time is spent on unplanned work? And unplanned work isn't free, right? The more time we spend on unplanned work, the less time we have for the completion of planned work. So that results in another key metric, cringe which is project due date performance.

And the highest contributors to unplanned work are around outages and availability. So the best indicators there in terms of operational performance is change success rate, in other words, what percentage of changes work the first time with the desired outcomes? And when things blow up, the first fix rate measures how good is your organization at having a culture of causality and fixing things the first time as opposed to blindly rebooting things? And both of these lead to great operational characteristics as well as great information security characteristics.

Julia Allen: Well Gene, as always, it's been a real pleasure catching up with you and talking about I think this really foundational work that hopefully our readers and listeners will find useful to their endeavors. And I thank you so very much for your time.

Gene Kim: Julia, it's always a pleasure. Thank you.