The Security ‘X’ Factor
Transcript

Part 1: The Study

Stephanie Losi: Welcome to the CERT 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 Stephanie Losi. I am a journalist and graduate student at Carnegie Mellon, working with the CERT Program. I am pleased to introduce Gene Kim, Chief Technology Officer of Tripwire and co-founder of the IT Process Institute. Today we'll be discussing the critical role of change management in security and the study that confirms this. So, Gene, welcome.

Gene Kim: Happy to be here.

Stephanie Losi: Thank you. What I would like to ask you is, change management has played a large role in your career, ranging from the development of Tripwire to your recent work on prioritizing IT controls. So what initially led you to identify change management as a vital focal point for security?

Gene Kim: I think there were a couple pivotal moments where we kept on gravitating towards this area. One was since 1999 we have been studying a group of high-performing IT operations and security organizations that had the best service levels as measured by mean time to repair, mean time between failures; best security as measured by earliest and most consistent integration of security into the IT operations life cycle; the best posture of compliance as measured by fewest number of repeat audit findings and the fewest amount of staff dedicated towards those compliance activities; and then the fourth characteristic was that they were also most efficient, as measured by high server-to-system-administrator ratios and low amounts of unplanned work.

So we co-founded the IT Process Institute really to try to capture and codify what is it that these 11 high-performing organizations were doing differently. And so that led to a project that we called the Visible Ops work, where that really codified the transformations of how those organizations became great, and specifically compared it to all the transformations we had seen fail—the hundreds, if not thousands, of organizations that have tried to transform but never reached the end result. So we published that in 2004. And after that we stepped back and asked the question, "Is Visible Ops correct?" Right? That one of the two things that we posited was that what made these high performers different was they all had a culture of change management and a culture of causality. So we had this great desire to bring a little bit more empirical rigor to IT management and IT security management.

Stephanie Losi: Right. And so these 11 organizations, how did you select them? How big was the pool to start with, and how did you identify these particular organizations?

Gene Kim: Yeah. It took many years to kind of come up with the crisp criteria, but they were all talking differently, acting differently, and had these radically phenomenally better results. So we actually came up with quantitative measures of these things. And what was amazing was they came from all different industries, all different company sizes. Essentially they had all independently, Darwinistically, came up with the same operational run book, essentially each to prevent the last disaster from happening again. So one of my favorite quotes is, "Behind every FAA regulation is an airline crash."

Stephanie Losi: So what kinds of incidents were you seeing that spurred them to really make these changes?

Gene Kim: Yeah. That is a great question. They were all high-profile outages, catastrophic incidents of unplanned work, late projects, as well as security incidents. And so our goal was to really say, "All right, is it true that a culture of change management and a culture of causality is what really discriminates high performers from low performers?"

So in 2004, we started a project called the IT Performance Control Study, which is really designed to say, "Hey, there are many good things that you can do, ITIL process frameworks, COBIT control frameworks. But what they all sort of don't cover is, where do you start? These are all sort of like dictionaries. Organizations don't do dictionaries. They do projects, right? So our goal was to say, "All right, let's see if we can test all of them, just like a pharmaceutical would do with a drug trial."

So we took the six leading areas in ITIL that people said "here is where you should start": access management, change management, configuration management, release management, service level management, and resolution processes. And so we decided to test all of them. We picked 25 control measures spanning from ops measures to security measures. And we benchmarked 98 organizations over the last three years, and the goal was really to come up with better answers to, "What are the rewards of high performers in terms of performance measurements? What controls do high performers do that medium and low performers don't?" And I think there were two huge surprises that came out of this that was incredibly illuminating. The first surprise was how good the high performers were. We expected a performance difference of 2X. What we found instead was that high performers consistently outperformed their peers by a factor of 5 to 8X.

Stephanie Losi: That's a lot. Okay.

Gene Kim: Oh, that is amazing.

Stephanie Losi: So what was causing that to happen?

Gene Kim: What was different in the performance was that they were doing 8 times as many projects. They were managing 6 times as many applications. They were implementing 7 to 14 times as many changes. When they were making the changes they had one-half the change failure rate, one-quarter of the first fix failure rate, five times higher server/sys admin ratios, and, incidentally, higher budgets—three times higher budgets.

There are two explanations, right? One is high performers are high performers because they have more money, but I think the more persuasive argument is IT has two jobs: deliver new projects to the business; operate and maintain what you have. And what we find is that low performers can't do either, and so therefore they can't get budgets to do anything. Incidentally, the security difference between high performers and medium and low performers is almost the same: 5 to 8X. What percentage of security incidents result in a loss event? High performers it was like one-fifth. What percentage of security incidents result in a loss? About one-fifth. And again, three times higher budgets between high performers and low performers.

The second big surprise is, what are the high performers doing differently? We found out of the six ITIL processaries, the 63 controls that fit them, there were two controls that every high performer had that none of the medium and low performers had. So, in other words, they were universally present in high, universally absent in medium and low. And those two things were: Do you monitor systems for unauthorized change, but just as important is, do you have defined consequences for intentional and unauthorized change?

Stephanie Losi: Interesting. Okay. And so the first one fits right back to Tripwire, so obviously that was of great interest to you. So when you looked at these conclusions, what did you think about them, and did you communicate these findings to the organizations?

Gene Kim: Oh, absolutely. They say the goal of science is to explain the most amount of observable phenomena with the fewest number of principles, confirm deeply held beliefs, and reveal surprising insights. And I think that the two discriminate controls—monitoring systems for unauthorized change and defining consequences—really, when you hold that up against the light with Visible Ops, I see a culture of change management that says tone from the top. Whoever is at the top of the organization says, "Change management is so important to us that the only acceptable number of unauthorized changes is zero. And we're not going to manage by belief. We have to manage by fact, and we're going to hold people accountable to that, and we're going to put controls in place so that we can find variance before causes or production outage, or security incidents." I think it definitely validated some beliefs that we have strongly held. But I think more importantly it simplified what is important, and I think helps the management focus on what is keeping them from being high performers.

Part 2: Taking Action

Stephanie Losi: What would you say to a company that really doesn't have a change management process in place right now? How do they get there? And then how do you enforce that down in the trenches as well, because it's one thing to say, "Well, there will be no unauthorized changes," and another to really enforce that when someone is under pressure and they have a deadline coming up, and they need to get it done.

Gene Kim: Exactly. Oh, in fact, how many times have I heard that? Absolutely. "Our business is so dynamic that we cannot—suddenly we have to break the rules." Right?

So the way that we need to coach the CIO to sort of keep the organization on the wagon is essentially by having them publish three things. One is a list of all scheduled authorized changes. The second was a list of all unauthorized changes. The third one is, what are the consequences and the ramifications to that person who made those unauthorized changes? And so working with the audit community, if you can imagine, this is going to be the plan that they would put IT management on, and the goal here is to say, "All right, the declaration is good. Now prove to me on an ongoing basis that you are actually following these procedures." And I think what is just so neat about auditors is kind of the third step, which is: Trust is not a control. Hope is not a strategy. So what we are going to do is we are going to look for all unplanned outages. Really, the theory there is that behind every outage—unplanned outage—is a failure in the change control process. So where would we look if we want to find evidence that the change control process really isn't working? Just look for the outages, and that is very hard to hide.

Stephanie Losi: And I have a question for you about why you think change management turned out to be such a strong determinant of overall security performance? We've seen that it is so important to get it in there to become a high performer, and that you have to really kind of tackle it from the top and get the tone from the top all set, and then make sure it's enforced in the trenches. So if an organization is going to go through this, is going to tackle what could be a significant project to really change the culture of the organization as regards this, I think they should understand why do you think this turned out to be such a strong determinant.

Gene Kim: What a great question. In fact, this is still something we are still really trying to gain an understanding of, but I think if you look back far enough in the security theory, the people in the old electronic data processing age, they would say there are three places where security must hang their hat. One is access controls. Do only appropriate people have access to computing infrastructure? The second one was change. Are all changes being controlled in a way that makes sure that you're not drifting into some uncontrolled configuration state? And the third one is a fallback, is business continuity. Can you bring back and restore service when it goes down at inopportune times?

I think what we're seeing is that when you look at high, medium, and low performers, you don't get the breakthrough in performance until you tackle change. I found two security executives who went into organizations and saw that there was no change control process, and they made the determination that their success hinges on having control over changes, and so they created the change management process, which is something I had never seen before. So I think it confirms deeply held intuitions for the practitioners decades ago, and we can even see how it is influencing security executives now. So, to answer your question, I think it's one thing to keep bad people away from business infrastructure, but in order to really make sure that you have a baseline, that you do not drift to a baseline, that security has to be a part of the change approval process, and they have to know when someone is circumventing the controls, because if you don't have control over change, then you really do not have control at all.

Stephanie Losi: This is only coming out recently, and it seems to be a really strong finding in terms of the results of the study. We have known about access controls for years. I mean, there has been almost this obsessive focus on passwords and smart cards, file permissions, making sure only authorized users can access the resources they are supposed to access. Now, why do you think there is such a focus on access controls versus change management, especially as change management proved to be the determining factor in this study, and how would you propose shifting that in the larger security culture?

Gene Kim: Oh, boy, another great question. I think the reason that security gravitates towards access controls is typically they are in complete control over it, kind of the issuance and revoking of entitlements and access, provisioning when business users are hired or fired. The link to change management is not often as strong in the job descriptions. And so I think we see two things happening. One is that in the high-performing organizations there is always some champion for the change management process, and when that exists, they own the prosecution of unauthorized change. So the instant an unauthorized change is made, essentially if operations doesn't prosecute that to completion, then it becomes security's responsibility.

I think what we're seeing now is that when organizations don't have that champion for change management process, security executives are actually stepping up and saying, "Hey, in order to be secure, in order to have timely detection of variance before it causes a loss event, we need some sort of change management process." So they're actually willing these processes into being and, going back to the benchmarking findings, providing not only huge security benefits, but also huge operational benefits as well—more projects, more changes, better change success rates, better first-fix failure rates, higher server/sys admin ratios, I mean, I think, evidence that security is helping improve daily operations.

Part 3: Overcoming Hurdles

Stephanie Losi: All right. Let’s say an organization is implementing a change management process. What are some of the likely hurdles they might encounter? Do you ever find that there is resistance among employees to this idea, or do they tend to just go along with it? And if there are hurdles, how can an organization overcome them?

Gene Kim: Yeah. I think the biggest hurdle is the perception that change management is bureaucratic, slows things down, and sucks the will to live out of everybody it touches. When we look at the benchmarking findings, we find that this is absolutely not the case. They are getting more projects done. They are getting more changes done with a higher change rate, and they are getting less unplanned work due to failed changes.

So I think there are three common misperceptions that are quickly formed by the organization. One is, "We can't enforce a change management process because we need our people to be creative. They are like precious birds. You can't put them in a cage." And I think the mis-thinking there is that building cars is very creative, but you can't have people moving equipment around on the production line. Second one is, "Our people are too highly paid for us to micromanage." I think what we find is that when you deal with something as mission critical as IT, the worst thing that can happen is for you not to have control, and you look at the difference between high and low performers. But I think the third one is maybe the most interesting to me, which is that it's always easier to draw pretty process diagrams on whiteboard or implement a technology. At a certain point management has to really earn their pay and figure out, "What do you do when Joey keeps making unauthorized changes?" At a certain point, management must make the call that, "Hey, the risk is so high around this, we have to put Joey in a role where he cannot make changes anymore." It doesn't mean firing him, it just means putting him in a role that's more suited to his temperament.

Stephanie Losi: So if an organization has implemented change management but is not seeing any improvement, do you think some of these things might be at the root of that, or might it be other issues? What might be wrong, and where would you tell the organization to look based on your experience with change management rollouts?

Gene Kim: Great question. So I think the benchmarking findings can help us there. I would look for the top two controls. Are they present? Do you have tone at the top as defined by defined consequences for intentional unauthorized change? The second thing I would look for is, are you enforcing a change management process to do controls, or is it just a meaningless binder on the bookshelf?

The second thing is I would look for metrics where, if you are doing change management right, you should be able to see immediate improvements around. One is number of unplanned outages. Every time you have an unplanned outage, that is a failure in the change control process. So if you are doing the right things, you're not going to have these 2:00 a.m. all-hands-on-deck situations.

Stephanie Losi: Everybody would like not to have those.

Gene Kim: Absolutely. The second thing is look for reduction in mean time to repair. What you want to see is—80% of all issues are caused by change—so you want to see people ruling out change first in the repair cycle, not last. And then one of my favorite metrics is change success rate. What percentage of changes actually work the first time and happen on schedule? And we find that high performers have change success rates of over 90%. Low-performing organizations sometimes as low as 50, 60%.

Stephanie Losi: Right. And that is because of their change management process.

Gene Kim: Absolutely. Right. In fact, it is very difficult to bring your change success rate up to over 50, 60% without having some control over how you're making changes. And the enterprising, ambitious person might also even look at first-fix rate. What percentage of your fixes worked the first time, so when you have an incident or an outage or security incident, how many of your restoration procedures actually worked the first time? Best-in-class is again 90%, worst-in-class is 50% or below.

Stephanie Losi: All right. Thank you very much, Gene. This has been great. Do you have any resources that you would point leaders to if they are considering implementing change management in their organization? Where should they look? Where should they go just to kind of get a background on this before they get started?

Gene Kim: Absolutely. You can find the Visible Ops Handbook at the ITPI website. That is itpi.org. In fact, you will see Julia Allen is the person who wrote the foreword to that. And the other work that Julia Allen and I worked on is the Change Management Audit Guide through the Institute of Internal Auditors. And you can find that on the iia.org website.

Stephanie Losi: Thank you very much. It’s been a pleasure having you.

Gene Kim: Thank you.