Ensuring Continuity of Operations When Business Is Disrupted
Transcript

Part 1: The Increasing Scope and Importance of Business Continuity Planning

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 web site. My name is Julia Allen. I'm a senior researcher at CERT, working on operational resilience and software assurance. Today I'm pleased to welcome Gary Daniels, Vice-President and Director of Corporate Business Continuity Planning for Marshall and Ilsley Corporation. Today Gary and I will be discussing the critical role of business continuity planning in support of operational resiliency.

For our listeners' information, Gary has been working with CERT for several years in developing and piloting the CERT Resiliency Management Model with several of his colleagues in the financial services sector. So welcome Gary, really glad to have you with us today.

Gary Daniels: And thank you Julia and I hope this will be very interesting for all you listeners.

Julia Allen: I'm sure it will be. Well let's get started. For just by way of introduction, could you say a little bit about the scope of business continuity and, particularly in your role, why it's becoming more and more important?

Gary Daniels: OK and if I can just go back a little bit. Business continuity, disaster recovery, and even services continuity were all terms that were widely used throughout the industry – all meaning the same things and everybody just used it interchangeable. The problem with that is that prior to 9/11 it all meant data processing. Everybody planned on how they were going to get their computer rooms up; how they were going to get their computers, their networks, the information back online. Business continuity though today really includes the data processing portion, which is technology; it's the computers. It also protects the information of the system and the facilities, the workstations, and the people assets. Today you have to include all four in business continuity; you can't just do one of the four.

If you focus on technology for instance, and not the people and facilities, you'll get your systems back up, you'll get your information back up. Now you've got nowhere to go or you have no people that can get your services back up for your customers. And that can cause you a problem. And then on the other hand, if you don't protect your data, and yet you have a place for the people to go, but now you have nothing to run, nothing to use. So business continuity today really is so important because it's going to keep your business running, and keep it afloat, and you want to keep servicing your customers.

Julia Allen: You know that makes good sense because when you think about if some kind of a disruption occurs, it could minor, it could be major, it could be a natural disaster. You've got all dimensions of the business to contend with, right? You've got, like you said, facilities, people, information, technology. Why do you think from a historical perspective that the emphasis was on technology or IT?

Gary Daniels: Well I think in the past, especially in the financial arena, so many banks outsource their technology to service bureaus. So, they kind of forget about doing disaster recovery or business continuity. And they just left it to the outsourcer. And that really isn't the right thing. Even

if you outsource, no matter what industry you're in today, you need to plan for your facility, you need to plan for your people, you need to plan for your services. Your role in a company is to service your clients or your customers. And if you can't do that, you're going to be out of business.

Julia Allen: So it sounds like it's also really important to apply to your outside service providers the same rigor, the same criteria that you apply to yourself right?

Gary Daniels: Correct. And I think later we'll talk about that.

Julia Allen: Great. So considering the audience of our podcast series, let's talk a little bit about the relationship between business continuity and information security. Could you say a little bit about that?

Gary Daniels: Well you know the interesting part of that, one of the four major assets that we want to protect is information. Business continuity folks have a very difficult time doing that without the input from the information security personnel. So we work very closely in understanding what they do and they work very closely with us to ensure that what we are doing is correct. But first you got to think of it this way. You have recovery plans that protect the storage of the information -- in other words your facility, your hardware, your infrastructure. You want to make sure that's all there to protect that information. Then you have recovery plans that really cover the firewalls, the encryption to ensure that if you have to activate a recovery plan, that same firewall or that same encryption is done at your alternate location. And then the third point really is at your recovery location, you want to make sure that you have the same physical and information security set up that you would at your main facility. So in other words, if you have secured (your) facility with card access or pin number access or bio(metrics) access, you want to make sure that at your alternate location you have almost the same set up. And then if you have a certain kind of access for doing transactions in your system, you want to make sure that you don't open it up at your recovery site and allow employees now to do anything they want. You want the same securities set up in both areas. So you need to work very closely with the information security groups to make sure that is continued from your normal location to your recovery location.

Julia Allen: OK, so in essence you're saying you want to have the same controls in place if you have to go to an alternate site, or even if you have to maybe shut down certain parts of your primary facility and just operate others, you want to make sure those controls are all consistent right?

Gary Daniels: Correct.

Part 2: Determining What to Protect; Identifying Key Players

Julia Allen: OK, so that's a lot to protect. That's a lot to undertake from a planning and allocation of resources point of view. So given that you can't protect everything (or probably it doesn't make good business sense to protect everything at the same level, particularly under times of stress, or in the face of disruption), how do you advise the business to best determine what processes, what services, what assets are most essential when you're doing continuity planning?

Gary Daniels: Well, that's interesting how you started because most companies in the past plan for every type of outage. They have lists and lists of what could happen and what are their plans to recover. And you can have mechanical problems, you can have facility failures, you could have weather failures if your company is in multiple regions of the country. So now you've got to plan for hurricanes in the south, you've got to plan for snow in the midwest, in the north. You plan for mudslides, rain in the west. I mean you just have so many more scenarios to plan for. And then,

you can even expand to that if you're an international company. Now you could have civil disturbance in different countries that could cause your business to be interrupted. It's really hard to plan for all of them. So if you have a good plan, you should be able to plan for a total outage, and then you should be able to implement only the parts that pertain to the outage. And that makes your planning a lot easier. And then some companies actually form a business continuity steering committee that would help you prioritize your business units. And then when you do have an interruption, those are the first business units that you activate.

Julia Allen: OK, so this is kind of interesting from my point of view because in the work that we're doing, we really focus on the asset or the service. And what I heard you talk about is there are many, many different scenarios that you have to prepare for. And do you find that the planning process takes more of a scenario or outage view? Or does it tend to take "this asset is really critical or this service is really critical regardless of what the source of the disruption is? So we've got to put these controls around the asset." Or do you do both?

Gary Daniels: Well no, it all depends. When you talk about people from an emergency response, we do it where we try to give them more scenarios like weather that could affect their regions or events that could affect their regions. When you talk about recovery of a business unit, we do look at the business unit as an asset. And we prioritize which business units are the most important to the organization and those are the ones that we have to get up and running first. We don't do scenario planning where there was a fire, where there was a chemical spill, where there was a power outage. To us, we can't operate, we have to move, we have to get the business back up and running and that's our decision.

Julia Allen: OK, so regardless of the disruption right?

Gary Daniels: Correct.

Julia Allen: OK, so let's talk about some of the players in this enterprise-wide endeavor of business continuity. So who are some of your key internal and external stakeholders that need to be really involved from the very beginning?

Gary Daniels: Well you need to start right at the top. And that is with your executives and your board of directors. If you don't have their buy-in, it is very difficult to get the business unit owners to buy into your program also. Because if you think of it, business continuity doesn't bring in revenue; it's an expense, it's overhead. And if you don't get the buy-in at the very top, you're not going to get the buy-in at the other levels.

As I stated before, forming a steering committee to help you prioritize which business activities are more critical to the company and how do you prioritize them to make sure that those are the ones we want to come up first with. You also can have crisis management teams. And what this is is a team of a key individuals throughout the company that when an outage occurs, they get together and they can then make the recommendations -- should we declare disaster, should we relocate people, should we just wait it out and see how long it's going to be? But they know exactly how an outage or a long term outage could affect each one of their business lines, and they would help make that decision for the company. And then one of the most important parts there is the line of business manager, or their liaison, focusing on the recovery of their business units. Those are the people that we have to get to, to write the plans and make sure they're done correctly.

And then what you need to do is once you get the buy-in, you need to really put together governance for the company. And the governance is really a definition of a program, the policies, responsibilities of all the different people within the organization, whether it's the executive, the

crisis management teams, whether it's your recovery teams, or your line of business participants. And then really what you should do after you have governance in place is start your recovery plans and then conduct your exercises.

Julia Allen: You wanted to say something perhaps about working with your external parties, your vendors. Are they part of this planning process?

Gary Daniels: I would say they're the second part of it. I would say get your own company together, get your plans together. Once you have those going -- if you remember when you define a recovery plan, you're going to be defining your critical suppliers, the inputs to your process, which are your vendors. And you want to make sure that those vendors participate in your exercises or you participate in their exercises to make sure they really can recover if they have an outage to keep supplying you. On the other hand you want to make sure when you have an outage that they can get their supplies or their support to you at another location. So they're just as critical as having a plan for yourself.

Julia Allen: I'm kind of curious, what have you found -- I mean some organizations I assume the folks at the top understand that this is just a natural result of being in business, this type of planning exercising, what have you. So do you find that you're able to get the time and attention from your steering committee members, and from your line of business managers, or is that challenging?

Gary Daniels: I would say 5 years ago, I would've told you it was very challenging. Today, as there are more interruptions to business, whether they be like a 9/11, whether they be an earthquake, possibly a wildfire in the west, or just power interruptions. We seem to have more and more power interruptions daily at different facilities around the country. I think the awareness of it is so much greater today that we do have the support. I have the support all the way to the board where I give annual presentations on our recovery planning, our governance, to make sure they approve it. So we have great buy-in it at this company.

Part 3: Developing & Exercising a Business Continuity Plan

Julia Allen: So once you have this stakeholder group in place, you've got your executive sponsorship buy-in, you've got your various committees and teams established, can you briefly walk us through the steps of actually developing a business continuity plan?

Gary Daniels: Sure. What we do is once we have the steering committee prioritize the different business units -- those are the ones we want to focus on first, the mission critical ones -- and you want to make sure that you develop a business impact analysis. And what that is is just a group of questions, it could be 10, it could be 30, it could be 50, it doesn't have to be a lot, but you want to ask questions to find out how much revenue they contribute to the company. If there is an outage, what would that do to the impact of them delivering service to the company? So you want to know really the history of this business activity or business unit, so then you can prioritize them. And then once you have that, you then go ahead and you develop templates for recovery plans and have the business units fill them out. And what you want to include in the recovery plan is on call notification procedures. You want to make sure there's a damage assessment procedure there. And then you definitely want procedures on how you're going to recover at your alternate site. But one of the bigger things you need is identify what systems, what workstations, or how many workstations, what vendor requirements you need -- really the assets that you're going to need at their recovery sites. So they're there ahead of time if you're able to do that, if they have a live recovery site for you. And then once you do that, you start testing the plan.

Julia Allen: OK, so and I think that's obviously a very, very key point. I mean you can plan all you want but you need to have some level of confidence or some level of assurance that the plan that you've developed is really going to stand up when something bad happens. So can you say a little bit about exercise and test how you get that level of assurance that you're in pretty good shape?

Gary Daniels: Sure. What you need to do is if you develop your governance, you need to define in there what is the occurrence that you should be testing your business units. Now something that is mission critical could be tested twice a year, four times a year. Something that is, I'm going to say, non-essential to your organization. It's there and maybe it's only tested once a year. Maybe it's tested once every 2 years, because the function is maybe an oversight function. It's not day-to-day service provider to your customers. So based on the priority, you might have different testing requirements.

Now once you start testing, you need to consider this as a normal department working somewhere else. So you've got to make sure that your alternate site is equipped to support that business unit. You've got to make sure that they have the, let's say, online access they need, the PC's, the systems at this alternate site, the correct security at that alternate site. And then you need to add any applications that normally reside on their desktops at their home location at the alternate site.

But then you could be a help desk where you have to reroute your phone circuits, and to make sure that the incoming calls are still allowed to go to this alternate site so you can service your customers. And the key then is to perform your daily functions and have security in place, both physical and regarding your information, to protect everything that's going on.

The one thing you have to remember is that in today's online processing there is so much corruption that once somebody has a disaster, it seems like the fraudsters know even more on how possibly to get into your backup systems, now thinking that you have let your guard down. So you want to make sure the security is there and protected also.

Julia Allen: So when you're actually doing the kind of process that you're describing, do you actually run it through its paces? Do you actually put folks at an alternate site? Do you do table top exercise, simulation? I mean and maybe it depends on the criticality of the business unit. How far do you go in actually doing a full exercise?

Gary Daniels: I think the answer to that is all of the above. But if you have a mission critical department, we would relocate the whole department. If you have what you'd call a vital department, you might relocate portions of the group to see if they can conduct the work. But when you have a mission critical (business unit), we actually let that department process at that location as it was their normal site. So again it all depends on the priorities.

Julia Allen: And I apologize. I kind of cut you off. Could you say a little bit more about this once you've had a disaster, the hacking community or the fraudsters know what your processes are. You may be a little bit in a weakened condition, so you have to be extra careful about your backup facility. Can you say a little bit more about that?

Gary Daniels: Sure. I think in today's world that there are so many people trying to break into systems. And try to make their system look like yours, so your customers give them all the bad information or the information that would make the fraudster look like a normal customer.

Once you have a disaster, that to me is just sending up the signals to all fraudsters to say, "Hey we have a problem. Maybe there's now an easier chance to get into the systems. They might have their guard down. They might not have all the security at their backup location that they have at

their main centers. And we possibly get into their system easier." And go that way. So again, it doesn't matter what industry you're in. I think the fraudsters are all trying to get into everybody's systems.

Julia Allen: So when you find yourself in the midst of one these events, I would imagine communications, public relations, how you manage the whole, how much information you let out, how transparent you are. That's a really key element as well right?

Gary Daniels: Correct. You would have -- you could form a communication team that would work with the media or work with the press to make sure that they got information out to the public on what the status of the recovery was, so your customers knew how to react or where to go to get the services you need.

Julia Allen: Well Gary, this has been really a great introduction to a very complex subject that needs to be carefully managed at the enterprise level. Do you have some places where our listeners can learn more?

Gary Daniels: Well I think one of the things you can definitely watch for more webinars and podcasts like this one. You could go to web sites like "Disaster Recovery Journal" or "Disaster Recovery Institute." There's a couple of other ones like "Contingency Planning Management", "Contingency Insights." Those are all web sites that would help you learn about what you should do. It's not going to tell you step 1, 2, 3, 4, 5 and how to put a plan together, but it's going to be sites that you can get information on. And then also each of them have annual business continuity conferences where you can get together with people who are in that industry and you can learn a lot from their presentations and their seminars.

Julia Allen: Well Gary I so appreciate your time and your expertise and the great insights that you've offered to our listeners and I look forward to another conversation. Thanks very much.

Gary Daniels: Alright, thank you.