# Integration with Third Parties

## Table of Contents

- Integrating Systems and Data with Third Parties ................................................................. 2
- Integrating with Third Parties - 1 ....................................................................................... 4
- Integrating with Third Parties -2 ..................................................................................... 5
- Interoperability Agreements ............................................................................................... 8
- Types of Interoperability Agreements .................................................................................. 9
- Integration Considerations -1 ............................................................................................ 13
- Integration Considerations -2 ........................................................................................... 15
- Notices ................................................................................................................................. 16
**040 Instructor: Today you cannot get away from working with third-parties. It's not possible. Especially with cloud computing. We're reliant on a lot of other organizations for our data.

You can tell very easily, on a personal level, how married you are to the rest of the planet and third-parties by turning off your internet connectivity for a day-- that means your phone and that means your wireless-- no internet-- and see how many things that you actually go to do that can't get done. This becomes very important also in an enterprise standpoint. If we lose the internet
connection, what systems stop functioning?

Now, some will function for a short period of time internally because they have some sort of caching mechanism here. But eventually there will be a failure. And so we have to know how we are integrated with other organizations and how our systems integrate with theirs.

One of the things I see a lot is our backup strategies have now been outsourced across the cloud. For small and large businesses today, they're using things like Dropbox as a backup or as a synch of a second copy of a particular set of files. I know that's not an enterprise solution, but people are using it as an enterprise solution, thinking that it helps them and backs them up. You'd be surprised at how many people don't realize that they're using Google Drive or Dropbox, or any one of the other tools that's out there.
Integrating with Third Parties - 1

Introduces an increased risk of data compromise

- Sharing of data and trust

Only as strong as your weakest link

Need processes in place for integration

**041 What happens is when we do that, our risk goes up. Operationally we are dependent upon somebody else. Now, if you just lose your internet connection for a little while, that's fine. But what happens about the dependency on top of the dependency? You also have to look at the processes for integration. Let's say you decide to outsource all this to some sort of infrastructure-as-a-service organization. What kind of processes are in place, like change control, change management, patch management, and which pieces of those are you responsible for?
Integrating with Third Parties -2

Integrating with Third Parties -2

On-boarding/off-boarding business partners

• On-boarding – Process of giving new business partners access to systems
  — Are both companies’ security policies compatible?
  — Who is responsible for what data?
  — Are there legal privacy or other regulatory requirements?
• Off-boarding – The closing of a business relationship

Social Media Networks and/or Applications

• Who has access to business accounts?
• What material can be posted? And where?
• Impact of compromise

**042 When we have business partners that we're relying on, this is an entirely different thing. Suppose externally they use some sort of infrastructure, platform or software as a service, and they say, "We're going to provide this service to you. You're going to be able to order your parts online 24/7 without calling us, and all we provide you is a web interface, and it's ready to go." That new business partner, they're giving you access to their resources and you can be able to click on them.

Let's go the other way around. If you say you're providing service to them, what are your security
standards and responsibilities? Do you follow certain auditing processes for your security under the scope of this business arrangement between the two of you? If you have strong security and they have strong security, everything's wonderful. But when I say to somebody, "Is your security pretty strong?" what are they going to say? "No, we really suck at what we do. I'm sorry. You really shouldn't do business with us." They're not going to do that. They're going to go, "Oh, we blah, blah, blah. We do it all. Yeah, yeah, we got that whole redundancy thing down, because I heard about it in a magazine and I asked somebody if we have redundancy and they said yes."

Now, here's the reality of it. Their security posture and your security posture are going to be, in some way, shape or form, different. That's all there is to it. When you start trading information back and forth and you start integrating to each other, you've got legal issues, you've got privacy issues, you've got regulatory requirements that they may have to impose upon you because these systems are connected together, and that's potentially dangerous for you.

So when you integrate with third-parties, sometimes that close business relationship, you can't get out of it. But for corporations you can wiggle away.
Next is things like social media networks and applications. Do you use these to communicate with the outside world? For example, a lot of corporations today are actually creating their own accounts with all the social media organizations and they're actually manning them on a regular basis. My idea, which is happening more and more often these days, is that that is the point of contact with the individuals outside of your organization where they can ask for help faster than anything else.

I have actually seen an organization that is a marketing organization that mans social media for a very, very large airline, and they have a person that sits at the desk and looks at all the different social networking and has a filter for everything that is toward that airline. When somebody complains that there is a problem with their seat or they can't get on the plane or there's a delay or something's going wrong, and they start squawking very loudly about it, and it starts to trend on one of those social networking sites, immediately those people create an alert and they send it to a marketing individual within the organization to go back and squash that clamoring. It's pretty amazing that they actually do that.
Interoperability Agreements

Interoperability Agreements

Formal contract that defines some form of arrangement where two entities agree to work with each other in some capacity

Outlines the specifics of any exchange or sharing of services

Wide range of forms and types of agreements

**043 Interoperability agreements. When you're dealing with these people, when you're dealing with these other organizations, the requirements in the contract need to be very clear. I'm sure that you've all seen contracts where you just signed them and went on your merry way, but when your intellectual property is at risk, when the people that you're working for or working with internally in your company, you're risking them, you better read that contract and get it all out at the very beginning. Because if it isn't in the contract, it's definitely not going to get done.
When you talk about exchanging information with people, you talk about how they exchange that information. And every time that they make a new request, you have to look at it and say, "This is the specific way that we exchange and share services and share data, and here’s how we’re going to address it in this instance." There are all kinds of forms and types of agreements that are out there.

I mean, they’re very-- they’re all over the place.

**Types of Interoperability Agreements**

**Types of Interoperability Agreements**

Service Level Agreement (SLA) – an agreement between two parties where the level of service is defined.

Business Partner Agreement (BPA) – a contract between two entities dictating their business relationship. It defines the expectations and obligations of each party.

Memorandum of Understanding (MOU) – a letter of intent with a means to document the specifics of an agreement or arrangement between two parties (without legally binding them).

Interconnection Security Agreement (ISA) – a formal declaration of the security stance, risks, and technical requirements of a link between two organizations.

**044 Let’s look at a couple of them here.**
Service-level agreement. This is a contract to provide a service. And it usually talks in terms of time. "We will restore your-- we will bring your backup tapes to you-- with Silver-level service, we will bring them Monday through Friday 9 a.m. to 5 p.m. If it’s outside that service window, you’ll get your backup tapes the next business day."

Okay, I don’t want that. What’s my next level of service? "Okay, we’ll return it to you-- through Monday through Friday, we’ll return it to you anytime during that 24-hour window during those days, but when it comes to the weekends, you don’t have that contract." Okay, how can I get that? Now we’re moving up the food chain here and it’s getting more and more expensive. Management is going to make decisions based on this service-level agreement. Look at all the different ways that that can get done. Look at their standard contracts and really start picking them apart and see whether you actually want to go with one of these very large organizations or whether you want to look to a smaller organization where you can have more control.

The rule, by the way-- this is for everyone. This is for you and I-- he who writes the contract, she who writes the contract wins. Period. So hopefully you write the contract. But sometimes we don’t have a choice at that. If we’re buying from Amazon, we can’t write the contract with Amazon. They’re way too big, we’re way too small, in most cases.
Business partner agreements. Now, there's a little bit more here that's going on that causes problems for us. This is the business relationship defining the expectations and obligations for each party.

Then there's something that's a little bit wider here that usually covers a lot of the specific things. It's called a Memorandum of Understanding, or an MOU. These are the general principles that we will treat each other with. Like for instance, what is the jurisdiction for litigation? If we need to go to that. We put that in this MOU. We don't put that in our service-level agreement down here. What we say in the service-level agreement is, "There is an MOU in place and it holds off all of this stuff here." MOUs are usually wider, bigger things, and then we have specific SLAs in it.

Interconnect security agreement. This resonates with a lot of DoD people. How do we deal with each other? What is our risk stance? How do we connect to that network? What is the requirement when we're connecting to the JACO's network, or the SIPR or the NIPRNet? What are the responsibilities that we have to have in place and who assumes those responsibilities? That's just for the military people.

Interconnect security agreements between commercial entities, they get a little fuzzy. And so I want to offer up one solution for you all to take with you when you go back to
your corporate world. If my organization and your organization want to work together and we think that there's an inequity in the security here, how about what we do is we write up all the things that we want, what I call a high-water mark. "You want certain things at this level; I want certain things at this level." We both write that up, and don't inflict that on each other. Let's hire a third-party. "Hey, do our web server for us. Hey, do our SharePoint service for us. You have to follow all my rules, you have to follow all their rules, and this is the service level that we want from you."
Integration Considerations -1

Privacy considerations
- Protecting the confidentiality of PII

Risk awareness
- Both organizations must share information regarding risks

Unauthorized data sharing
- Can lead to the disclosure of private, confidential, proprietary data

Data Ownership
- Needs to be identified and delineated

**045 Now, let's look at some of the deeper, detailed things that should be in those contracts, if you will.

Privacy considerations. What is your personally identifiable information for your organization and how can we interact with that? A classic example of this is you have your organization set up under Active Directory, and if you look at an end-user, all these fields are typed in, and it fills out every single piece of information for the person, because Human Resources uses the Active Directory fields to issue out paychecks and all that stuff. If we decide to do federated identity between us-- in
other words sharing accounts using something like SAML connectors-- that's Security Assertion Markup Language-- we decide to do connectors between us to say, "Okay, your second-level administrators can create accounts for this particular organizational unit."

If that's the case between us, maybe we shouldn't be able to view that information. And you're going to have to set permissions in there to limit our view of that personally identifiable information. That is a privacy consideration. You've addressed it on your side; you've dealt with on your side; but we don't know about that, and so what we have to do is go, "Well, we shouldn't be looking at that data." But you should be making that decision.

Risk awareness. You'll have to get contractual acceptable of that.

Unauthorized data sharing: What will we do when it happens? How will we limit that?

Data ownership. When we’re finished, who gets the result of our property?
Integration Considerations - 2

Data backups

- Identify means of recovering data in the event of a loss or corruption

Follow security policy and procedures

Review agreement requirements to verify compliance and performance standards

**046 Data backups. When we're sharing data between each other, who's doing backups, who's doing verification? And the verification data must be sent to the other. So if you're backing up our data, I want you to verify that data and I want you to send me a report on that on a regular basis. Usually, for certain organizations, they have a compliance effort that requires them to have the receipts for that. It's not enough in audit to do it; you have to do it, be able to report on it, and retrieve that reporting statistic at a reasonable interval.
Notices

© 2015 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.