# Lessons in External Dependency and Supply Chain Risk Management

## Table of Contents

## Carnegie Mellon University – Notices

Carnegie Mellon University

This video and all related information and materials (“materials”) are owned by Carnegie Mellon University. These materials are provided on an “as-is” “as available” basis without any warranties and solely for your personal viewing and use.

You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced websites, and/or for any consequences or the use by you of such materials.

By viewing, downloading, and/or using this video and related materials, you agree that you have read and agree to our terms of use (www.sei.cmu.edu/legal/).





**053 ~Music Plays~

## Lessons in External Dependency and Supply Chain Risk Management

**October 14th, 2014**

CERT | Software Engineering Institute | Carnegie Mellon University

 1

**001 Shane McGraw: Hello. Welcome to the Software Engineering Institute's Webinar Series, coming live from Carnegie Mellon University in Pittsburgh, Pennsylvania.

Our presentation today is Lessons in External Dependency and Supply Chain Risk Management.

Depending on your location, we wish you a good morning, a good afternoon or good evening.

My name is Shane McGraw. I'll be your moderator for today. And I'd like to thank you for attending.

We want to make today as interactive as possible. So we will take questions throughout the presentation and again at the conclusion of the presentation.

You can submit questions to our events staff at any time through the Questions tab on your Control Panel.

We will also be asking a few polling questions throughout the event, and they will appear as a popup window on your screen.

Another three tabs I'd like to point out are the Materials, Twitter and Survey tabs.

The Materials tab now has the presentation slides in a PDF copy, along with SEI work in the area of Resilience and Risk Management and course offerings that CERT has as well.

The Survey widget will appear as a popup at the end of the presentation. We request that you fill that out, as your feedback is always greatly appreciated.

And for those of you using Twitter, be sure to follow @SEInews, and use the hash tag SEIscr; once again, it's SEIscr, as in supply chain risk.

And now I'd like to introduce our presenters for today.

Our first speaker will be John Haller. John is a member of the Technical Staff in the Cybersecurity Assurance Team within the CERT division of the

As a member of the team, John performs research on critical infrastructure protection, focusing on methods, tools and techniques for

managing external dependency and third-party risk.

Prior to joining CERT in 2010, John was analyzing cyber attacks on the financial industry, alongside a U.S law enforcement agency.

John received his Juris Doctor from the University of Pittsburgh, and is also a GIAC certified incident handler.

Matt Butkovic is a technical manager of Cyber Security Assurance within the CERT division of the SEI.

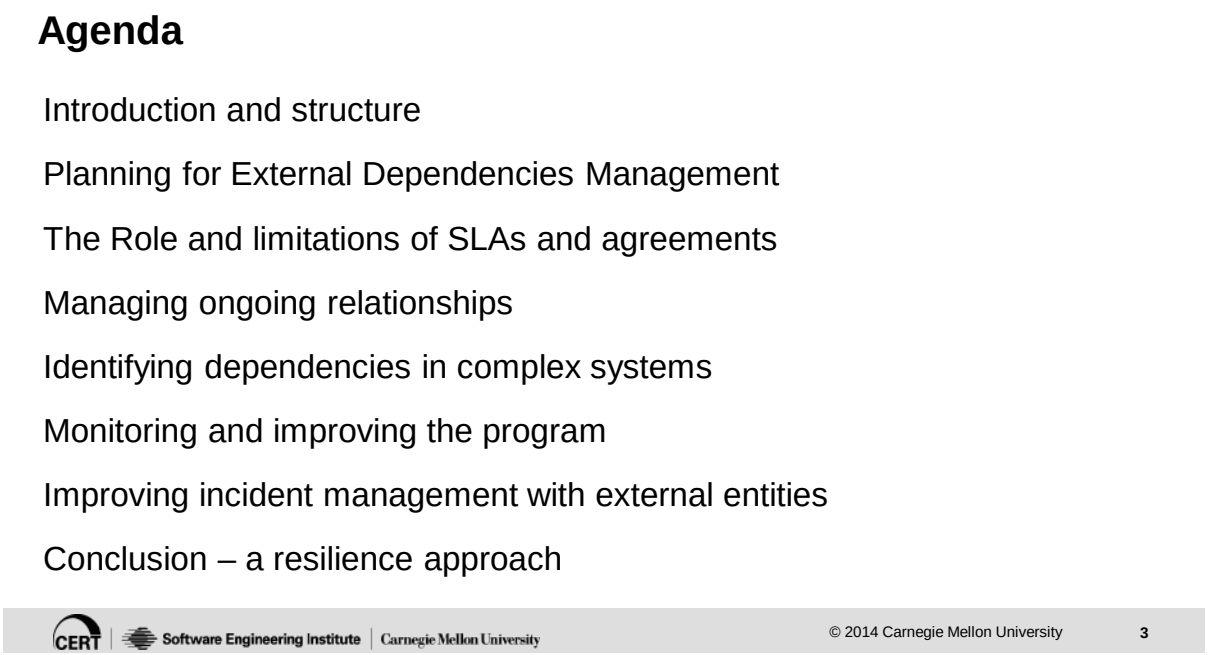
Matthew performs critical infrastructure protection, research, and develops methods, tools and techniques for managing risk. He has more than 15 years of managerial and technical experience in information technology across the banking and manufacturing sectors.

Prior to joining the CERT division in 2010, Matthew led information security business continuity efforts for a Fortune 500 manufacturing organization. He's a Certified CISSP and a CISA.

And now I'd like to turn it over to John Haller.

John, all yours.

## Agenda




**003 John Haller: Thank you Shane. Good morning; and thank you very much for your attendance this morning.

So I'm going to talk a little bit about our agenda. First of all, I'd like to mention that CERT will be sponsoring a Supply Chain Risk Management symposium in the Washington DC area, which will occur on January 15th of next year. So mark your calendars. We'd love to have your attendance and see you there, if you're in the DC area or you can travel to DC.

So I'm going to talk a little bit about the agenda for today and how we're going to approach this morning.

We're going to talk a little bit about the-- we're going to introduce External Dependencies Management

and what we mean by External Dependencies Management.

We'll talk about planning for External Dependencies Management; because a lot of our research has shown that- you know, obviously planning is a very important part of managing risk in this area.

Along those lines we'll, as part of the planning segment, we'll focus on the role and limitations of SLAs and agreements.

We're going to talk about managing ongoing relationships with external entities or third parties that your organization relies on. We'll look at a specific case study in that area; and we'll look at identifying dependencies in complex systems.

We're going to talk about monitoring and improving an External Dependencies Management program; what are some of the things that you would look at from an enterprise or organizational perspective to assess and improve how your organization is managing external dependency risk.

We're going to take a specific- look at a specific example in there, focused on incident management and exchanging information with vendors and other third parties.

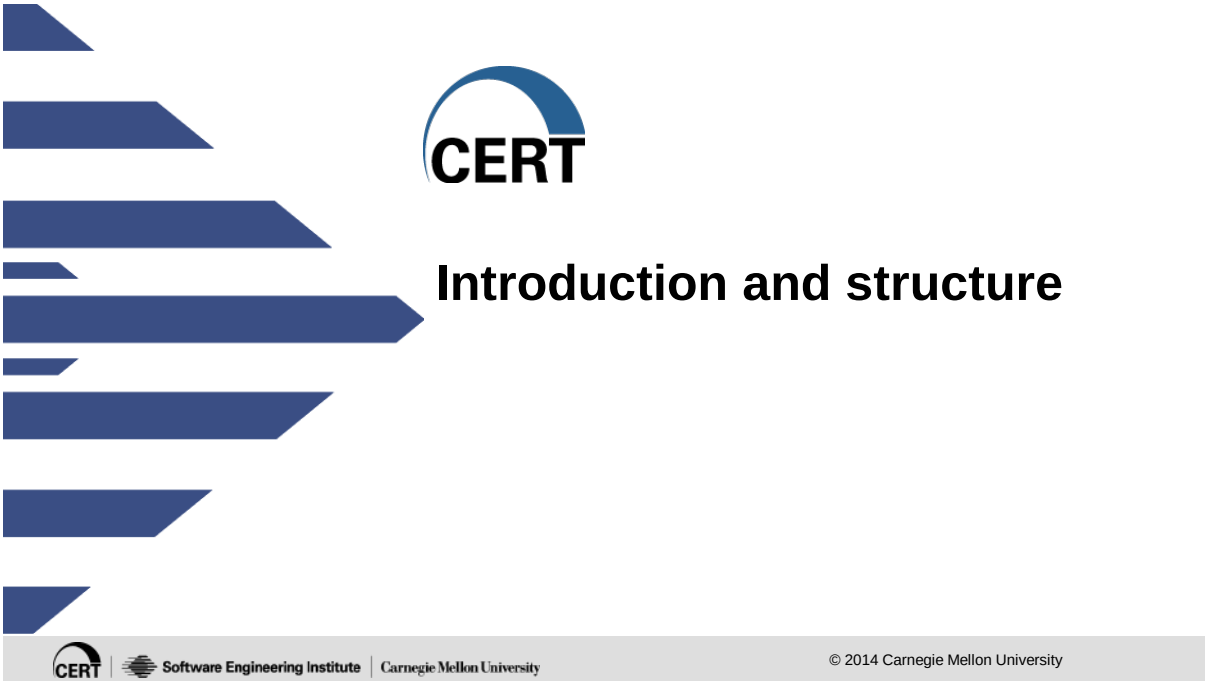
And finally we're going to conclude with an overview of a resilience approach. Matt, next to me, is going to talk a little bit about a resilience

view of third party and external dependency management.

Throughout this morning we're going to use two-- we're going to talk a little bit about two real-world incidents, and we're going to use them and take some examples from those incidents to drive our discussion in specific areas.

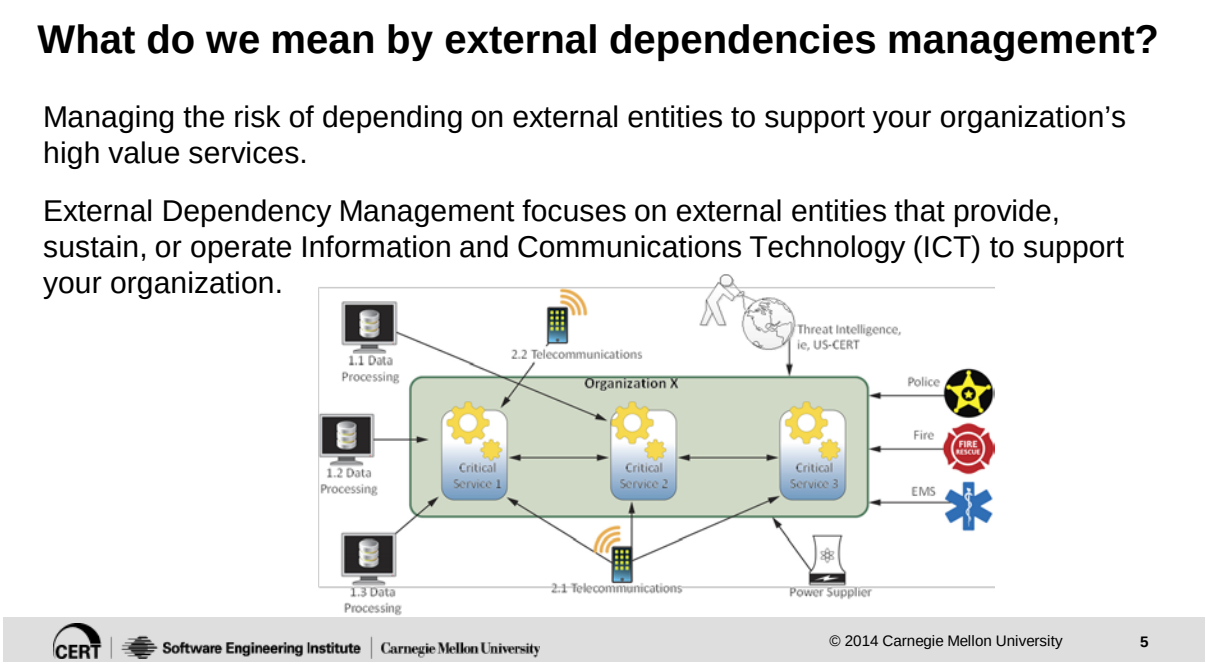
There's a lot of material here. We're-- so when we talk about planning, we're not going to go over every individual step. We're going to highlight certain things and provide certain takeaways for your organization.

## Introduction and structure




**004 So that you can improve your resilience with respect to third-party risk and external entities. Okay.

## What do we mean by external dependencies management?




**005 So we're going to talk a little bit about-- we're going to introduce the subject and talk a little bit about how we- how CERT and how we approach this.

Matt, over to you.

Matt Butkovic: Thank you John.
So let's explain what we mean by this concept of external entities and high-value services. Right?

We are-- today's talk will focus on ensuring that you have relationships with third parties that allow you to effectively manage risk and sustain relationships with those vendors and suppliers that offer services that are most important to your organization.

So think about this as the things that matter most from a productive

activities or mission perspective of the organization.

So you may notice that we're not- we're not speaking expansively about supply chain risk management in this webinar, though our work does encompass that. We're specifically focused on what we refer to as the ICT, the Information and Communications Technology facet of supply chain.

This is where a good deal of our recent work has been. So we're not suggesting that hardware provenance and other elements of supply chain aren't important. They very much are. And we will address that.

But for today's discussion we're going to focus on mainly services that are offered by a third party to your organization. And these can be the heart of your business; things you do at arms' length to do the things that matter the most for your organization.

John Haller: Yes I think it's important to mention that we kind of look at supply chain or external dependencies from a broad or holistic perspective. So it's not only vendors with which you have contracted relationships but any organization or any entity that you rely on to help you manage and use information and communications technology to provide what your organization provides.

A lot of the supply chain risk management discussion is really

focused specifically on vendors, where you may have a contract and you may have some ability to influence what that vendor does.

But it's kind of important to look at it more broadly because-- we'll talk about this a little bit-- one of the issues in this space is that sometimes organizations miss dependencies or fail to account for dependencies that really affect what they actually- what they actually provide. Go ahead.

Matt Butkovic: Sorry John. I was just going to add than when you think about this kind of comprehensively, you have to consider not only the relationships you have with third parties but the relationship those third parties have with other third parties. Right?

John Haller: Yes.

Matt Butkovic: So think of it as a sort of complex ecosystem of inter-related organizations. And we are suggesting that this is really an engineering problem; and like any engineering problem we have requirements and methods by which to quantify and manage the risk in that system.

John Haller: Right, absolutely. And Matt spoke to this a little bit. We're not focused specifically or exclusively on the provenance or source of hardware and software. But to some extent this is-- for instance, when the financial industry addresses supply chain or external dependency

risk, it's usually defined as third-party risk; third parties that a financial institution relies on to support the service. Other terms are of course supply chain risk management.

When we look at those subjects-- supply chain risk management and third party risk-- that all falls under the umbrella of External Dependency Management.

So for instance, if you're viewing this webinar and you work in the financial industry, when we say External Dependencies Management I think your organization would probably look at that as third party risk management. All the techniques and things that we're talking about are meant to address that space as well, or meant to address those concerns as well.

## Example incidents


**006 Matt Butkovic: I think that we would not have a proper webinar if we didn't have a list of scary things and bad things that have happened to kind of set the stage.

So on this slide is a list of examples of egregious things that happen when control is lost with third parties. And you can see the chronology of this, starting with Heartland Payment Systems in 2009 through Goodwill Industries in 2014. John will do a deep dive on the HAVEX and TRANSCOM events.

I believe that most of these events are probably known to the folks watching this webinar. But just a few things to note; some specifics that I think would add some context.

In the case of the Lowes breach-- and we're not picking on Lowes but

just an example-- there was a loss of names, Social Security numbers and driver's license numbers for store drivers. So these are employees of Lowes. Their PII is being lost by the organization. And this was the result of a failure.

A vendor offering something called E-Driver File, provided by SafetyFirst-- which is sort of an interesting name given the context. And the root cause of this was an improperly secured backup that created the breach.

So I think sort of one of the kind of interesting side notes is it's not always just sort of online information that can create a breach or create some sort of negative consequence. It's also things like backup tapes.

Another example that I think is interesting is the California Department of- sorry, the California Department of Child Support Services. Eight-hundred-thousand records were lost when backup tapes were being transported from an IBM facility to Iron Mountain.

And the quote is really interesting: "The cartridges are believed to have been lost in transit somewhere between Boulder and Sacramento." So that's a distance of nearly 1200 miles. And the supposition here is that the tapes are somewhere within that 1200 mile journey.

So not to sort of muddy the waters here. But something to think about

is not only sort of the online, on demand systems that we kind of- are front of mind when we think about third party relationships. But also think about the way those third parties are handling your data at rest, how they're handling backups and the full picture of the ways they interact with your information.

John Haller: Absolutely. So we're going to move to the-- I'm going to talk a little bit about two specific breaches in a little bit more depth: The HAVEX/Dragonfly attacks on the energy sector.

### Case study: HAVEX malware / Dragonfly






**007 And the DOD TRANSCOM contractor breaches that were just investigated by the Senate Armed Services Committee.

So we're going to use both of these incidents kind of as a driver. We're going to pull certain aspects of these incidents to provide some real world context to the things that we're talking about in the webinar this morning.

So this- the HAVEX- the HAVEX malware and Dragonfly attacks were published by or alerted by DHS's ICS-CERT in June and July of this year. And basically these involved attacks it is believed on the electrical infrastructure in the United States. And the attack method was basically-- it basically a watering hole attack, among some other methods used by the- used by the actors.

What they did was they corrupted and- they corrupted the software installers and control systems updates on manufacturer websites with a remote access Trojan, to be able to gain access to the organizations downloading the update; which in most cases were parts of the electrical industry.

Now again this was a watering hole attack. And what we're going to do is we're going to look at the implications of this type of attack for supply chain or external dependencies risk management.

## Case study: TRANSCOM


**008 And take a few lessons away from this, as we go through the presentation this morning.

So we're going to talk about TRANSCOM  a little bit as well.

TRANSCOM is the Department of Defense's Transportation Command. Their basic mission is to ensure the transportation and the movement of U.S. military assets around the world.

And it's probably not surprising to most of you in the audience that a lot this- a lot of this occurs on commercial carriers, commercial logistics companies; and that those commercial companies are relied upon to help move equipment and other assets.

So just a few weeks ago the Senate- the U.S. Senate Armed Services

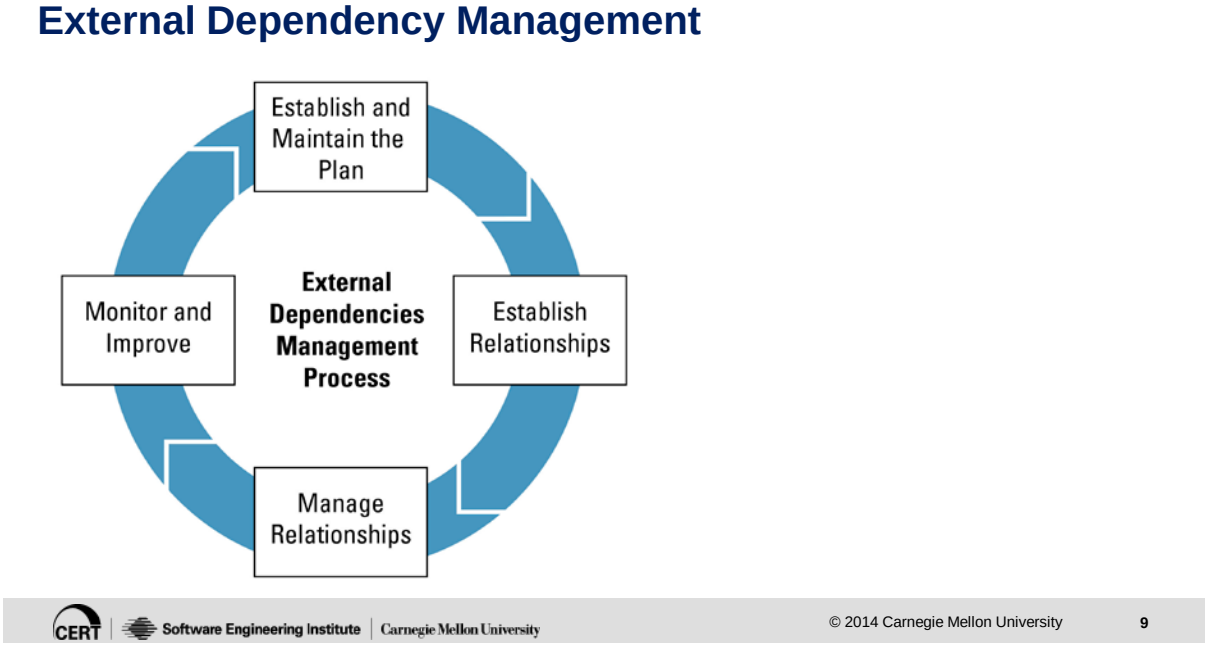
Committee publically released their investigation into this series of intrusions.

And what actually happened was a number of those private companies were- experienced security incidents and experienced intrusions; and there's some obvious incident management lessons there where it comes to third parties.

As it turned out, the actual DOD component was not aware of most of those intrusions.

And actually I would suggest for the audience that if you're interested in this, go out-- and it's freely available on the internet-- and you can find the report. Because there's a great- there's a- actually a postmortem and analysis of some of the third party terms and controls that were in the contract and how those were actually interpreted by the vendors and the external entities.

## External Dependency Management




**009 So it's actually very interesting reading. We're going to take a few lessons from this incident and talk about them today.

So this is kind of a-- this is how- one way to look at External Dependencies Management. The basic idea behind this is that-- probably not a surprise to people in the audience who are familiar with process improvement efforts-- it's essentially a feedback loop.

We're going to talk about some of the four components here in brief: Establish and- establishing and maintaining a plan for doing External Dependencies Management in your organization; establishing relationships with third parties or external entities; managing those relationships on time or over time; and then looking and assessing how

your organization manages external entities and what it could do to improve.

Matt Butkovic: John I was just going to say that I think that one of the takeaways I would hope from this webinar is that if you don't actively manage these relationships, you should have very little confidence that the things that you need to happen are happening. Right?

John Haller: Right.

Matt Butkovic: So we're not suggesting that third parties are trying to do things in a malicious or intentionally negligent way. We're just suggesting that things that you manage to a very specific requirement and actively monitor are far better off than things that are left neglected or under-examined.

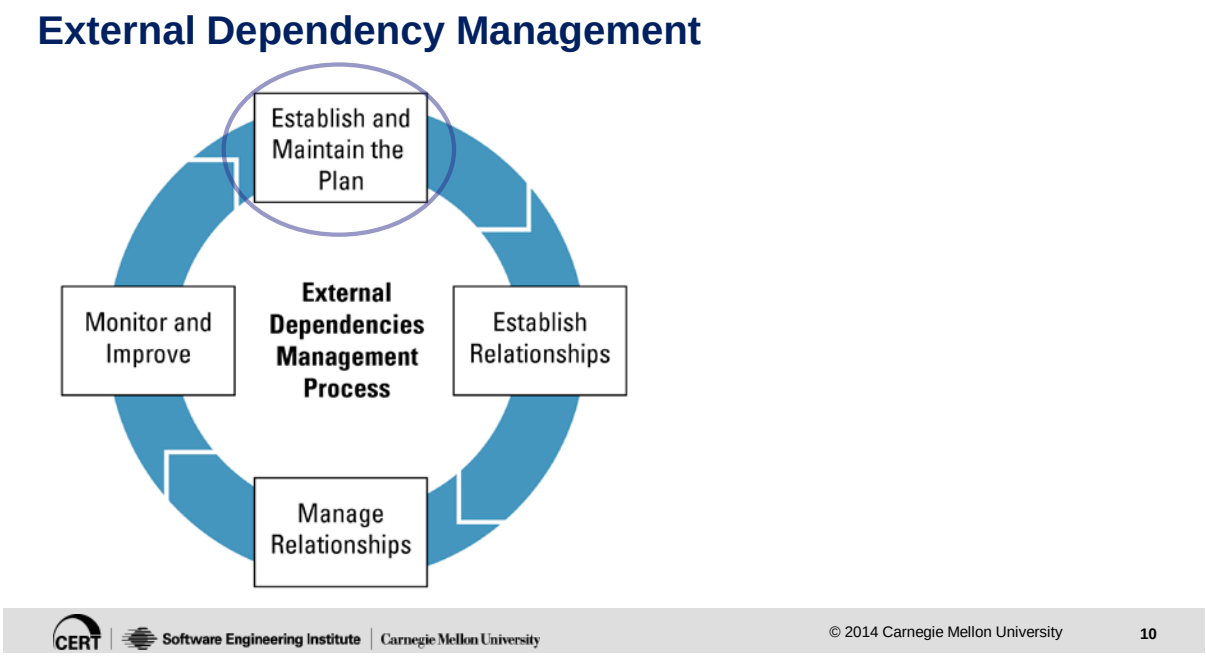
John Haller: Right, exactly right. And as we sort of go through this and look at monitor/improve, one of the other takeaways is that the organization for high-value services-- in other words things that your organization provides to its stakeholders that are of critical importance to the organization-- for those services you should really be looking and monitoring how well your organization is doing here and what your organization can do to improve external dependency management.

Matt Butkovic: And something that's implicit here is that the organization understands what those high-value services are.

John Haller: Exactly.

Matt Butkovic: So we're suggesting that to effectively manage supply chain risk you have to understand the things that are most critical to the organization; which sounds really obvious.

## External Dependency Management




**010 But we find that that some organizations really struggle to articulate and capture what the truly critical functions are in the organization.

John Haller: Yes absolutely right.

## Planning for External Dependencies Management

Key goals:

- Identify program management objectives
- Identify services
- Prioritize services
- Identify service requirements
- Identify enterprise requirements
- Plan relationship formation
- Plan relationship management

**011 So first we're going to look briefly at: Establishing and maintaining a plan for External Dependencies Management.

Okay. So the slide shows a few key goals in this area, a few things that your organization should think about with respect to standing up a program for managing external dependencies. And we're going to look at a few-- we're going to go into the planning relationship formation in a little bit more depth. But I'm going to touch on each of these briefly.

So the first one. If you're setting up a program in your organization to manage external dependencies, you should be thinking about what the objectives are for the program. What are you really trying to accomplish here?

Now a basic objective is to protect high-value services that the organization provides from third-party or external entity risk; I mean, that's a pretty straightforward objective- program management objective.

There are some others that in your organization may make sense or that you may decide to implement in your organization.

You know, with respect to managing risks from the source or provenance of hardware and software, I know the program management objective might be something like: We're only going to use trusted vendors or trusted distributors to provide or to buy the technology that we use to support those high-value services. That might be a program management objective. You know?

So something like this should definitely be considered by talking to the Legal Department in your organization; I mean, they might urge a program objective that includes something like forming relationships with entities in jurisdictions that are favorable to the organization from a legal perspective.

There might be a program objective about avoiding risks from political or third party- political risks if you're forming relationships with organizations in another country.

Matt Butkovic: John, I think it's also important to highlight that the

HAVEX situation I think illustrates very well the limitations of selecting vendors using that criteria; which is a reasonable criteria which is--

John Haller: Right.

Matt Butkovic: You want to make sure that you're dealing with a third party that's financially solvent, that's reliable; that provides the safeguards you're looking for. However that is not a guarantee you won't experience some sort of security issue once you establish that relationship.

John Haller: Right. I think that's a really good point.

So a lot of these- a lot of the activities that an organization might do here I think fall into the category of necessary but not always sufficient.

Matt Butkovic: Right.

John Haller: Right? It's a really good point; and we'll talk about that a little more in the HAVEX situation.

Next thing you want to think about is identifying services. Now when we say "identify services" what we mean here is identify your organization's services. What are the top three or four or five things that your organization does for its customers and stakeholders that are, you know, drop dead no matter what important for your organization to maintain and to protect.

Next we want to think about prioritizing services. Of those few things that your organization does that are critical to the organization, can you prioritize those and put those into some kind of order? This is a basic- a basic way to help drive management and resource allocations- allocation decisions in your organization.

The next thing is identifying service requirements. What are the service requirements for that critical service? In terms of confidentiality, integrity and availability, what requirements do those services that you provide really have to meet in order for them to be sustained and successful for your organization?

Next thing is enterprise requirements. These are requirements that should apply or would apply to any external entity that you enter into a relationship for certain functions.

Now kind of a basic; one example of an enterprise requirement is-- if anyone in the audience is in the healthcare field, a basic enterprise requirement for organizations that you contract with to handle healthcare information or electronic healthcare records would be the HIPAA requirements, if you're entering into an agreement with a business associate.

Now it's kind of important to interpret those requirements in your own context. But that's example- an example of something that's in that

case provided or given to the organization by a regulator that will impact and be an enterprise requirement for any outside entity that in that case is handling healthcare information.

Next thing is planning relationship formation. There's a lot of activities here.

But so some basic things in planning relationship formation; like who will the authorities be within the organization that actually sign off on contracting or forming relationships with outside entities?

What standards will the organization use to form those relationships?

How will the organization know if there are any changes to SOAs or contracts that might affect the- might affect the critical service?

And the last one we have on here is planning relationship management. After the- after the relationship is formed with an external entity or a vendor, how will the organization manage that relationship over time?

What will-- will there be reporting requirements that will be applied to the external entity?

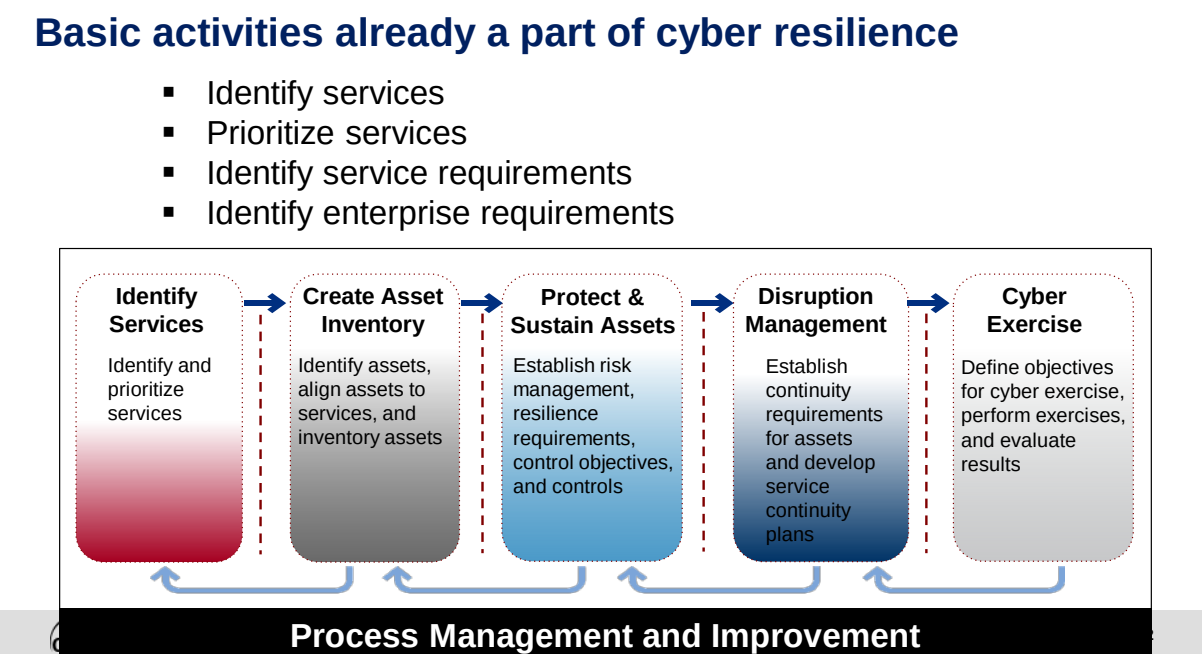
What will the internal reporting requirements be? Like if someone is dealing with the external entity or the business owner is dealing with the external entity, what kind of requirements will they have to report

information up to senior management- up to business managers?

And I actually think it's kind of important to remember that in that last section, planning relationship management, a lot of those requirements and reporting- reporting activity will not necessarily be documented in contracts or SLAs.

Contracts and SLAs are very important. However a lot of this activity may be outside the contract; and that's okay. There may be reasons that a vendor or a third party might not want to actually agree to that in a contract. But still it's something that- that's very important.

### Basic activities already a part of cyber resilience




**012 And that if they want to serve your needs they need to comply with.

So we want to talk a little bit about how this fits in with an overall resilience program.

And this is-- I think a lot of people in the audience might be aware that a lot of this work and how we look at it is related closely with the CERT Resilience Management model and trying to take a resilience approach to managing security, to managing service continuity, to managing cybersecurity generally.

What does that mean in this case? Well what it means in this case is a lot of those activities that your organization will do or should do to manage external dependency risk, those are also activities that generally fit into or are generally part of an overall resilience program.

So for instance basic things like what Matt was talking about-- identifying services in the organization, prioritizing services, identifying service and enterprise requirements-- those are things that the organization should be doing and really needs to do to manage many facets- facets of cybersecurity and resilience management.

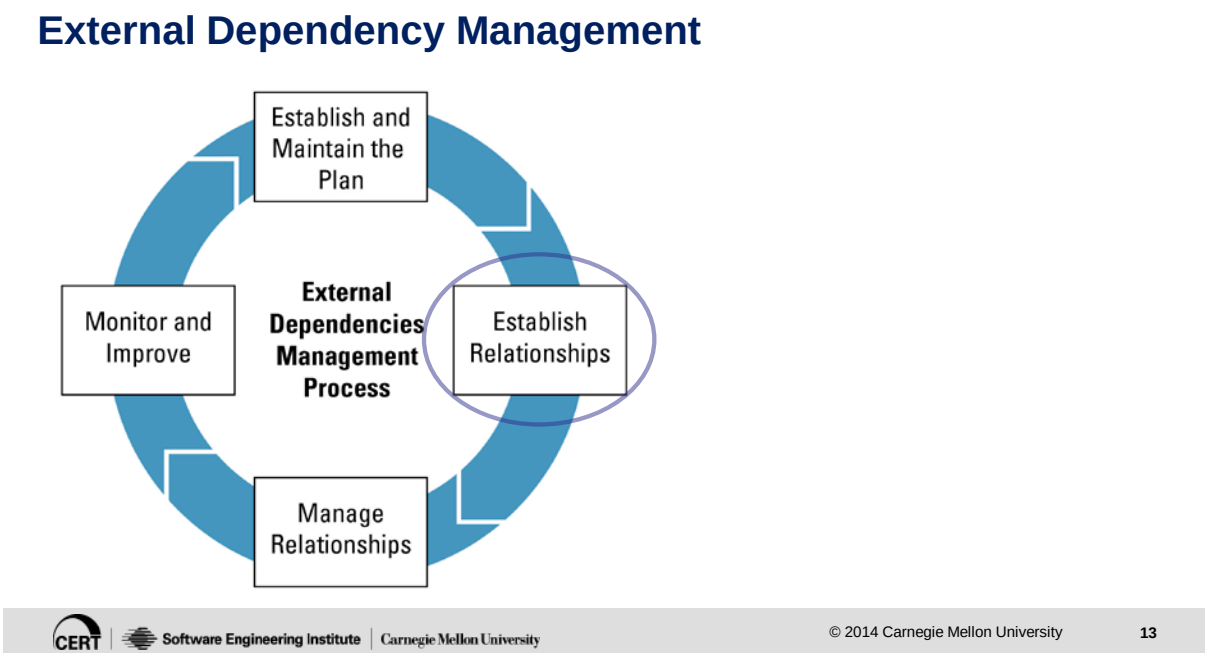
The idea is do once- do some of these activities once-- well not-- once is probably a dangerous term. Do these activities and apply them to different types of security and resilience issues. This shouldn't necessarily be stovepiped.

Matt Butkovic: So what's somewhat different, or actually in third-party relationships, is if you look at this kind of flow. When you think about creating an asset inventory, the assets important for these services may belong to a third- will belong to a third party. So it's a bit of a black box. You won't be able to enumerate them and manage them the way you do if they're within your own four walls within the organization.

So what I'm suggesting here is that this same model applies, the same process flow applies, wherever the nuances are, that these things will be done at times intentionally beyond your control; meaning the responsibility of a third party.

That doesn't change your obligation to manage the risk. You can outsource processes, you can outsource tasking. You can't outsource the fundamental risk to your organization represented by these relationships. And I think that's--

## External Dependency Management

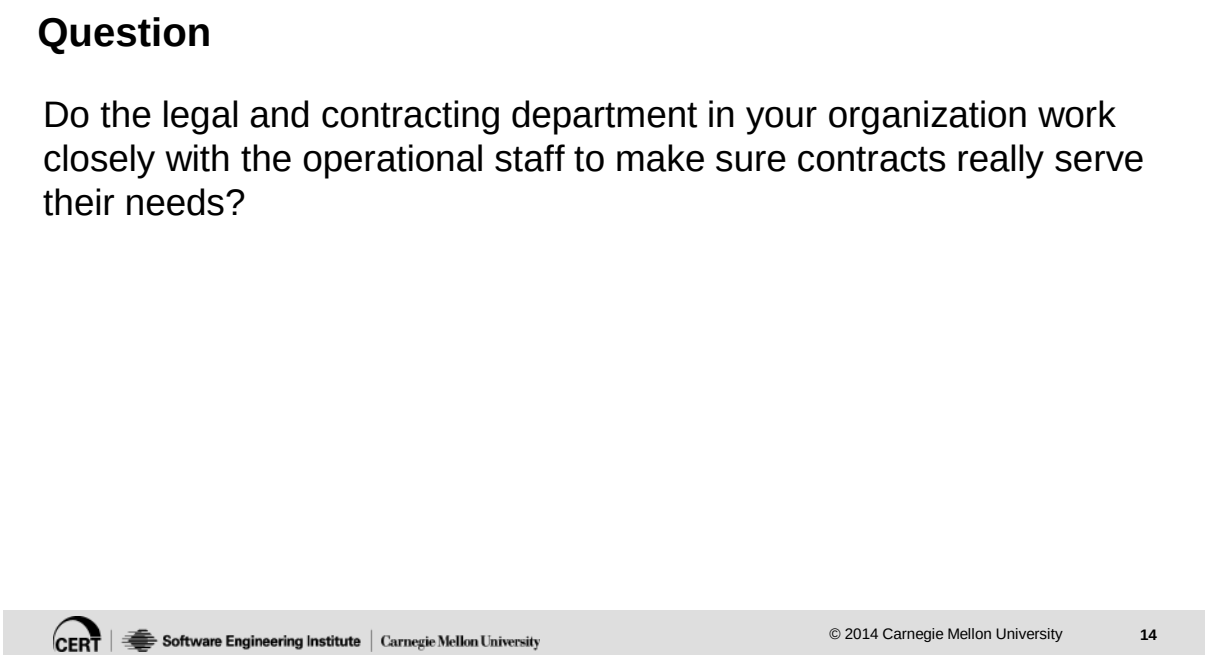



**013 You know, the fundamental takeaway in my mind is that at the end of the day that risk is still yours to manage.

John Haller: Yes absolutely.

Okay. So we talked a little bit about planning. We're going to move into some considerations involving establishing relationships.

## Question




**014 And Matt's going to talk a little bit about the roles and limitations of SLAs.

So first we have a question for the audience. You should have a window on your console or on your screen where you can type in your responses to this question.

The first question is: Do the legal and contracting departments in your organization work closely with the operational staff to make sure contracts really serve their needs?

So you can go ahead and input your responses to this. We're going to throughout the morning as we get responses and look at them. We are definitely interested in your interaction, your opinion, what you think are some real challenges in this space. So feel- please feel free to put those into your--

Shane McGraw: Right, just type them folks right into the Questions tab. This is not a full official polling question which will be a popup window. So we're just going to type it right into the Questions tab on your console. And as we get some responses we'll fill back in with that.

Matt Butkovic: Yes Shane, this is freeform.

Shane McGraw: Yes.

Matt Butkovic: So if folks have specific limitations in this regard they'd like us to discuss, please provide those; or examples of how integration between these functions and the people who are also responsible for the risk for these systems maybe has not been working well.

## Closer look: the role and limitations of formal agreements and SLAs

### Closer look: the role and limitations of formal agreements and SLAs

Organizations should:

- Establish and maintain requirements for external entities
- Include requirements in SLAs and other agreements
- Monitor performance against these agreements

Key point: Managers should understand the role and limitations of contracts and formal agreements





**015 Or what has been working well would provide a good example for us.

Shane McGraw: Yes.

John Haller: Okay. So Matt is going to go a little bit into SLAs and some of the limitations here and current trends in how this is being managed.

Matt Butkovic: So SLAs are essential. Right? So a Service Level Agreement is an absolute building block in this space. Right? This is something you need.

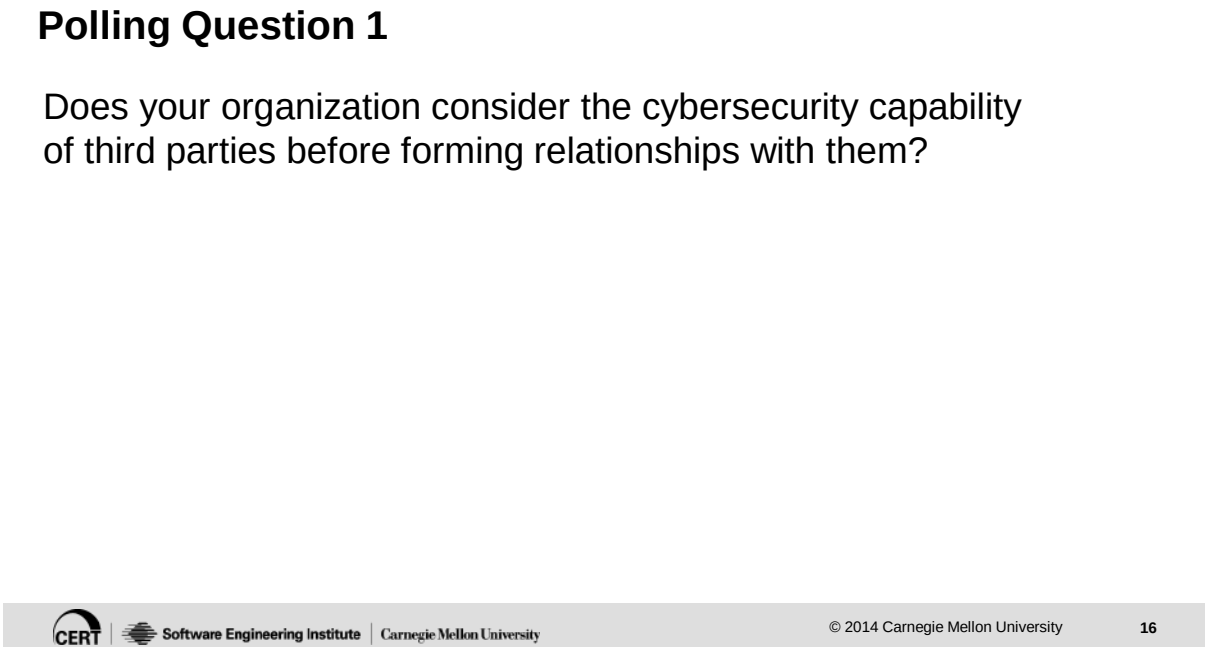
However it is not- it is not a defensive mechanism that will prevent a disruption or prevent bad things from happening operationally to the organization.

So we would advocate for creating SLAs; SLAs that make sense, SLAs that are measurable and enforceable. And then monitoring progress or monitoring performance against these SLAs is probably the most important facet of this.

So things like service reviews. Having dialogues with your third parties at some- on some periodic basis with an expectation that they'll be able to address the specifics of the SLAs.

Understanding at the end of the day the SLA is a mechanism primarily by which you can measure performance and then also seek restitution if something bad does happen.

### Polling Question 1




**016 They do not in themselves prevent bad things from happening.

Shane McGraw: Okay before we launch the first official polling question folks, we had a response from Denise to the question you had asked John. And her reply was: We work closely with our Legal Department to get security language into all applicable contracts.

Is that something you guys see normally? Is that the standard or is that abnormal that an organization is doing that?

John Haller: Well I think it's- I think it's obviously very good that Denise's organization does that.

I think that-- and Matt will talk a little bit about some of the- some of the responses and the things that we've learned during our field research.

I think it varies by industry in many cases and by critical infrastructure sector. There are some sort of critical infrastructure sectors that are tightly regulated, closely regulated, where they really look at this; and that is one of the first things that the governing body looks at.

What do you say to that Matt?

Matt Butkovic: So I think that-- it's a mixed bag. And having worked in organizations that have built this sort of language, and having assisted the Legal Department determining what was appropriate, I think it's a great thing to have.

One of the cautions I would offer is there's a temptation to make that language-- no offense to my colleague who's an attorney by trade-- but to make the language overly broad and basically not acceptable to the third party.

So I've seen- I've seen contracts that say: Thou shalt comply with ISO. Well ISO what? Right? Or: Thou shalt be secure. And then there's a lot of standards listed without some sort of-- more of what it is you want them to do.

So I think it's a great practice. It's definitely an essential element of this. I would just suggest to make sure it's understood by both parties and that it's measurable; and is not so overly broad as to just sap all meaning from it.

Shane McGraw: Okay folks so we're going to launch back to back polling questions which will appear as a popup on your screen. After we launch those questions, John and Matt will address a couple of audience questions; and we can continue on the presentation.

There are two questions, the first one being: Does your organization consider the cyber security capability of third parties before forming relationships with them?

## Polling Question 2

Does your organization always document security objectives in agreements with third parties that are critical to your business?





**017 And then our follow-up question to that will be: Does your organization always document security objectives and agreements with third parties that are critical to your business?

So I will launch polling question 1 now. And while you're voting we'll get into some audience questions.

A question from Don asking guys: On the breaches that you discussed, what SLAs failed or what SLAs were missing?

John Haller: I think Matt can address a couple of those.

What I would actually point people to-- we'll talk about this a little bit later-- is if you-- on the TRANSCOM incident.

If the audiences wants a really good example of SLAs and contractual requirements and how those were interpreted or in some cases not interpreted in a particular instance, the Senate Arms Services Committee Report that was publicly released, actually starting on page 33, is a really good snapshot of actual contractual requirements that were in place, and what the investigators looked at and reported on, how the vendors in that case actually interpreted those, in situations where they may have experienced incidents but did not report them up. On the other cases?

Matt Butkovic: Sure. So I think that it's-- there's a number of different situations in that list. Right?

So I think in some cases you could say that the third party lived up to the expectation of the SLA. However other circumstances created a really detrimental situation.

The Target breach is an interesting one from that perspective. So Target of course has a very- a very robust way of looking at vendor risk.

The breach that led to this billion dollar situation happened because a heating and cooling HVAC vendor in the Pittsburgh area, a third party, was given access to do some maintenance and monitoring of HVAC systems.

Now I'm gone out on a limb but I don't think Derenzo Heating and Air

Conditioning appears high on the list of vendors-- right?-- at Target; just based on the scale and size of relationship.

So I'd say in that regard-- I don't know what the contract looked like between Derenzo Heating and Air Conditioning and Target. But I would say that I'd be surprised if it had comprehensive language about cyber security.

So I'd say in that respect you have to understand that even the most unlikely sources of breach are out there; and that you should consider having some language in there to ensure that those- that everyone that's connecting to your network, interacting with your data or is part of this larger ecosystem has some comparable- minimal baseline of security standards.

Now I'm not- I'm not casting blame to any party here; you know, it was a very sophisticated attack in some ways. So-- sorry, I don't know if it's a very good answer for John. But I think that, you know, there's probably a paper in there for John and I to kind of explore the SLA failures within those breaches.

But in general, I can't point to one specific SLA or type of SLA that was not met or failures of that service level that led to those breaches.

John Haller: Well I think Matt brings up a really good point here; and this is something important in my

mind to think about when you think about SLAs and contracts.

That is one piece of the puzzle and one thing you do to manage an external dependency risk. I mean, you are basically trying to ensure that the third party is doing the right things from a cybersecurity perspective; and you're trying to drive their behavior with the SLA and get your organization some confidence.

However, there may be situations-- and we'll talk about this a little bit in HAVEX-- where that may not be that effective; and your internal processes around risk management, access management, all those basic things, kind of need to be looked at as well from the perspective of what can third parties do to or with your organization? Does that--

Matt Butkovic: Yes. I think there's also kind of mindset or perception issue at times; which is small organizations especially will say: We're handing this to a third party because we don't fully understand the situation. Right? We don't have the expertise to tell you what you should be doing security-wise.

Which is true. But I would suggest you should reach out for subject matter expert opinion-- right?-- or some sort of standard language that provides some understanding of what's appropriate security-wise in SLAs.

It's true. Right? If you're a very small organization, you're outsourcing many times because you don't have the talent, resources or time to do these things. However your exposure is the same as large organizations; maybe not from a financial perspective but to you it matters a great deal.

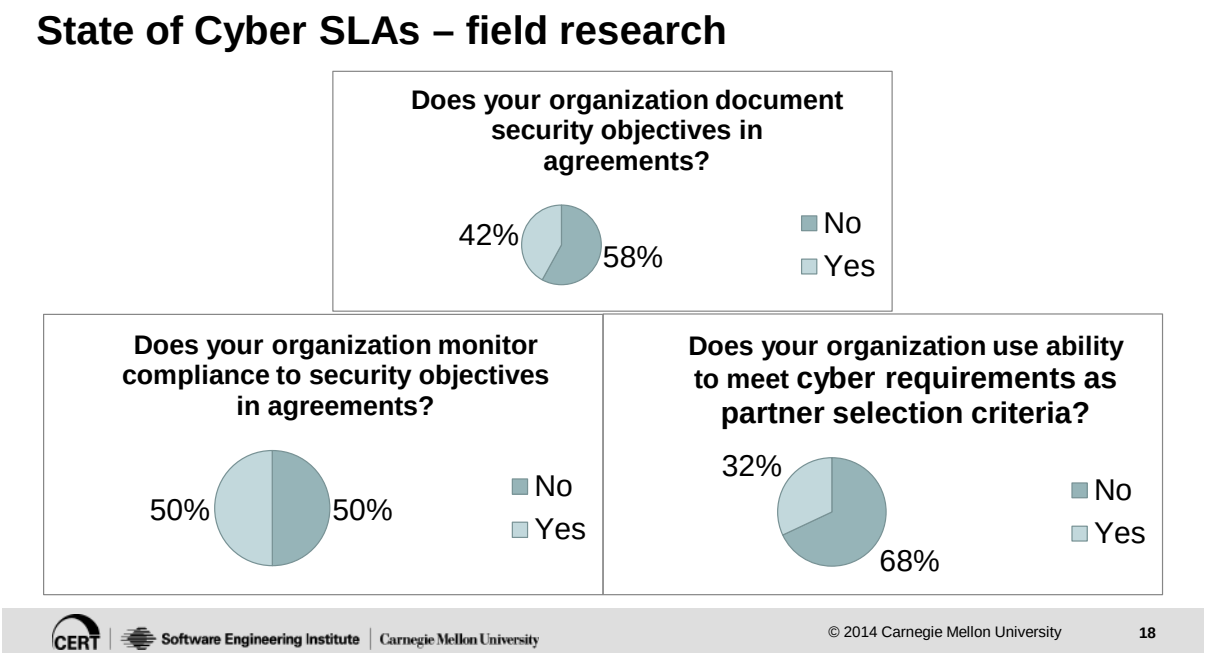
So I think one of the things that we can do to enhance the state of the practice, from the CERT side, is maybe provide that guidance or some understanding of what a minimum baseline in contracts or SLAs should be.

John Haller: Hum.

Matt Butkovic: So maybe in a follow-on webinar we can kind of explore what that would look like.

But I think it's important to note that no matter your size or scale, if you're putting something in the cloud, if you're using an out-source- using an out-sourcer..., these considerations exist for you...

## State of Cyber SLAs – field research




**018 ...as much as they do...

## Polling Question 2

Does your organization always document security objectives in agreements with third parties that are critical to your business?



**017 ...for the largest organizations we mentioned in the list of breaches.

Shane McGraw: Okay folks, we're getting a number of questions too about are the slides to this presentation available; and also a recording of the event?

The slides are available now in the Resource tab you'll see on your console. You can walk away with a PDF version, along with other materials CERT has offered in resilience and risk management.

Another question from Jim before we move on guys is: Do you use SLAs in federal government contracts; or is that more of a commercial industry practice?

John Haller: I think the lingo-- I can't say that I have an encyclopedic

knowledge of federal government contracting. I think the lingo may differ from the government side and the commercial side. But government components, government organizations certainly use things like SLAs and standard agreements to form relationships with vendors and external entities.

Matt Butkovic: Yes absolutely.

John Haller: I mean, that's-- you know? They do it.

Matt Butkovic: The terms may vary-- right?-- and the federal procurement language may be different. But SLAs are absolutely appropriate and expected when a commercial entity is interacting with a federal entity; or even federal entity to federal entity.

I would suggest that SLAs, although they're contractual in nature-- if you sort of take the ITIL mindset, you also have the ability-- right?-- to-with OLAs to also have that sort of granular understanding between operating entities within the same organization or between organizations that are not necessarily in a commercial relationship.

So I guess the short answer is yes I would expect SLAs, even in federal contracts.

John Haller: Yes, yes.

Shane McGraw: And just to put a wrap on our polls real quick. The

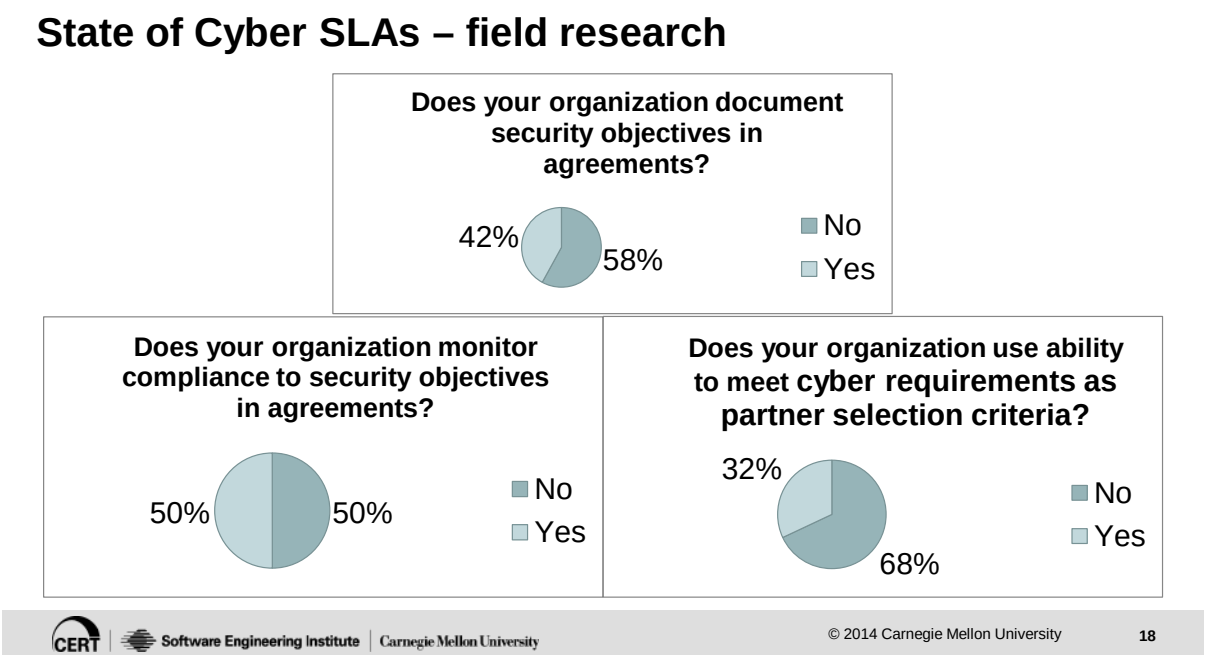
first polling question was: Does your organization consider the cybersecurity capability of third parties before forming relationships with them?

Seventy-nine percent responded yes; eight percent, no; and 13 percent, sometimes.

John Haller: Hum.

Shane McGraw: And for our second polling question-- which was: Does your organization always document security objectives and agreements with third parties that are critical to your business?

## State of Cyber SLAs – field research




**018 Seventy-one percent yes and 29 percent no.

John Haller: Okay that's good.

All right, so Matt is going to talk a little bit about some actual field research that CERT has done in this space.

Matt Butkovic: Sure. So I think the good news is it's kind of a self-selecting audience. You'll notice that the numbers that Shane gave for the participants on this webinar, the people answering Yes are quite a bit higher what we found.

So the chart in front of us here, these are- these are numbers that we gathered performing cybersecurity assessments for one of our- one of our important federal customers or partners.

So these are actual assessments of organizations. In this case there's around 150 organizations that comprised this study.

You'll notice that for the first question-- Does your organization document security objectives and agreements?-- 58 percent of those organizations we visited said No and 42 percent said Yes. Which is quite different from 77 percent of the folks on the webinar saying that they do that. So that's encouraging.

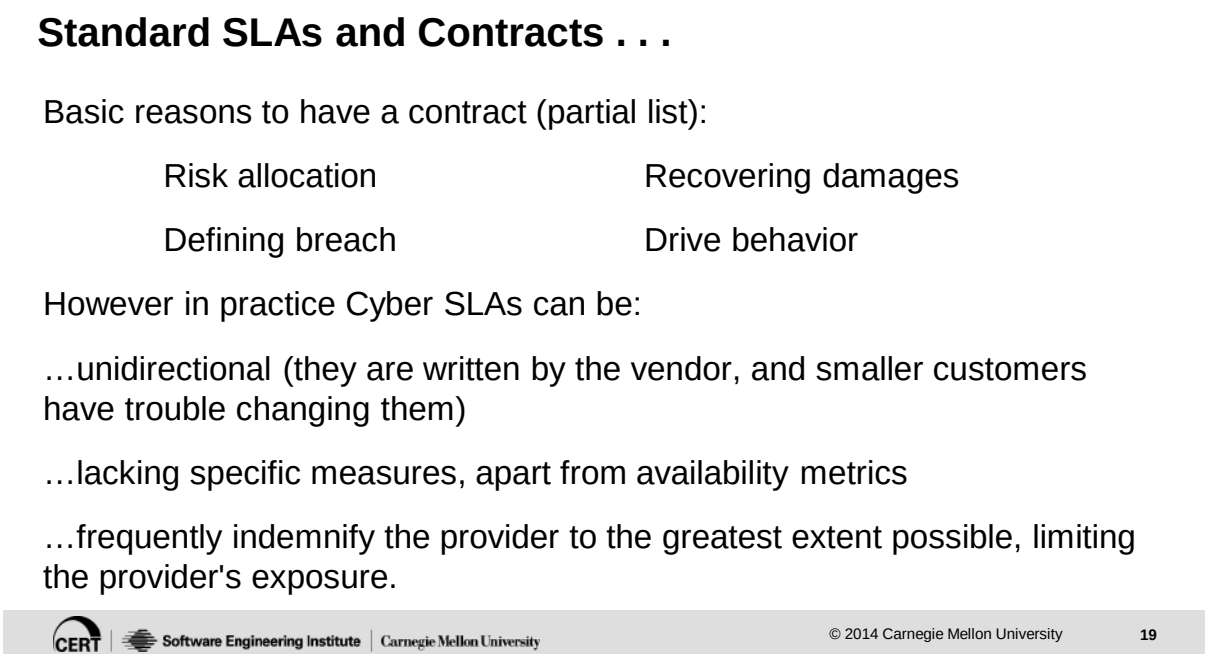
And then: Does your organization use the ability to meet cyber requirements or cybersecurity requirements as criteria in partner selection? Seventy-nine percent of the people on this webinar said Yes;

whereas 68 percent of the folks said No in the assessments that we performed.

So I think that the 13 percent Sometimes is really the more interesting stat Shane and John. But-- and this was my experience when I was in private industry-- that based on the size or scale of the relationship, you kind of scale your expectations SLA and security-wise.

But I would caution you to think about that Target example where an organization who's not overtly engaged in cyber security or systems administration, or even housing your data, led to a very detrimental situation.

### Standard SLAs and Contracts . . .




**019 John Haller: Absolutely.

So we're going to talk a little bit and go into a little more depth about SLAs and contracts. And I just wanted to mention to Matt-- but I figured you would out me as a JD; so I was sure that to list that in my bio and preempt you.

Matt Butkovic: That's fine.

John Haller: Okay.

Matt Butkovic: I think the quantity of description around things probably confirmed that without the bio.

John Haller: That's probably true, yes.

So we're going to talk a little bit about SLAs and contracts. We're not suggesting-- and I think Matt just echoed this very well. SLAs and formal agreements are absolutely a part of managing external dependency risk, of course; and there are good reasons for that. Right? There are a lot of basic reasons to have a good contract with your external entities.

Contracts in many fields are used to sort of allocate risk. You know, defining breach is another sort of obvious example.

If you're in a relationship with a vendor or an external entity, and you want to know what standards are supposed to be held to and whether or not they've failed on those standards and on their performance, you refer to the contract. It should be defined in the-- breach- breaching

the contract should be defined in the contract.

It has certain obvious- obvious relations to recovering damages. And it's ultimately supposed to drive behavior for the other contracting party.

But I think the-- I think in the information security and sort of cyber space they're at-- I would call it an immature state of practice. And Matt's going to talk about that a little bit more.

Matt Butkovic: Sure. So when you look at cyber SLAs, they're often unilateral. So they're often written, especially the large providers, as you might expect providing maximum benefit to the out-sourcer; which is an issue, especially if you are a smaller customer and you have very little sway over the relationship.

They often lack specificity. So good SLAs will have very specific measures; things you can count, things you can graph, things you can take into that service review and point to the pluses and minuses of the relationship.

And as I mentioned, they indemnify the provider to the greatest extent possible; which is- which again we're not saying is good or bad. This is just the nature of a competitive free-market system. Right? Which you-- you want to ensure that you maximize the upside and minimize the downside.

## Examples of Cloud SLAs - Amazon

"Reasonable and appropriate measures"

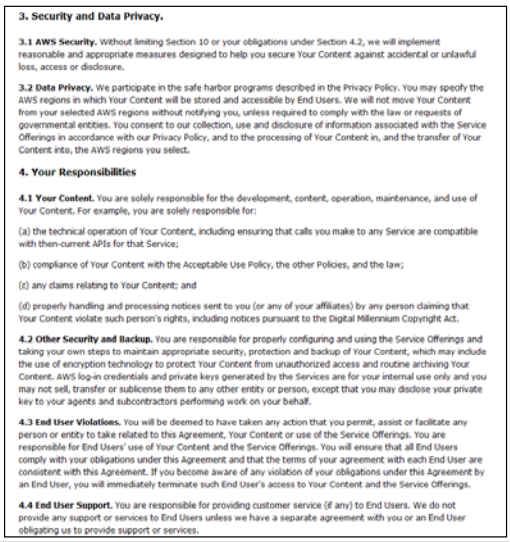
- no specifics
  (cannot use to hold accountable)

""You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security…"

"Limitations of Liability"

- Amazon not responsible for damages

-http://aws.amazon.com/s3-sla/



**3. Security and Data Privacy.**

**3.1 AWS Security.** Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

**3.2 Data Privacy.** We participate in the safe harbor programs described in the Privacy Policy. You may specify the AWS regions in which Your Content will be stored and accessible by End Users. We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities. You consent to our collection, use and disclosure of information associated with the Service Offerings in accordance with our Privacy Policy, and to the processing of Your Content in, and the transfer of Your Content into, the AWS regions you select.

**4. Your Responsibilities**

**4.1 Your Content.** You are solely responsible for the development, content, operation, maintenance, and use of Your Content. For example, you are solely responsible for:

(a) the technical operation of Your Content, including ensuring that calls you make to any Service are compatible with then-current APIs for that Service;

(b) compliance of Your Content with the Acceptable Use Policy, the other Policies, and the law;

(c) any claims relating to Your Content; and

(d) properly handling and processing notices sent to you (or any of your affiliates) by any person claiming that Your Content violate such person's rights, including notices pursuant to the Digital Millennium Copyright Act.

**4.2 Other Security and Backup.** You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content. AWS log-in credentials and private keys generated by the Services are for your internal use only and you may not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.

**4.3 End User Violations.** You will be deemed to have taken any action that you permit, assist or facilitate any person or entity to take related to this Agreement, Your Content or use of the Service Offerings. You are responsible for End Users' use of Your Content and the Service Offerings. You will ensure that all End Users comply with your obligations under this Agreement and that the terms of your agreement with each End User are consistent with this Agreement. If you become aware of any violation of your obligations under this Agreement by an End User, you will immediately terminate such End User's access to Your Content and the Service Offerings.

**4.4 End User Support.** You are responsible for providing customer service (if any) to End Users. We do not provide any support or services to End Users unless we have a separate agreement with you or an End User obligating us to provide support or services.

CERT | Software Engineering Institute | Carnegie Mellon University



20

**020 Just don't let that happen at your expense is what we're suggesting in those relationships.

John Haller: Right.

Matt Butkovic: So we're going to look at a specific example here. And this is just a kind of random selection. We're not suggesting that the organization named here is good, bad or in any way different from their peers.

But what I find interesting in this cloud SLA is terms like "reasonable and appropriate measures"; which is certainly not specific. And I think if I approached John and said, "We need to- we need to consider suing for damages" that'd be a very difficult starting point.

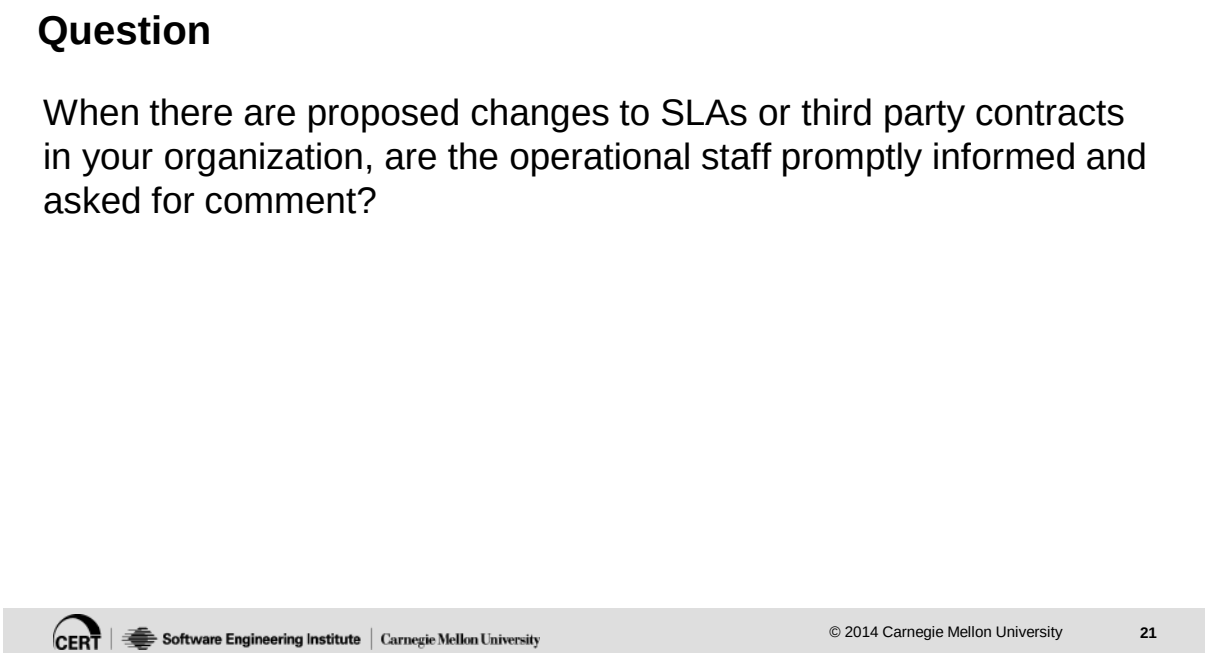
John Haller: Mm-hm.

Matt Butkovic: Now I should also mention this is stock language. And what you should do is of course push for language that's more advantageous and more beneficial to your organization when you're negotiating these things.

I think it's also interesting that in many of these cloud SLAs the obligation to identify a breach or a problem actually rests with the party receiving the service.

So it's not as if in the stock form in many of these cloud SLAs or cloud contracts that they're going to notify you that there's something wrong. It's up to you to tell them. And then you usually have a window. It can be a month or two months; or in some cases you have up to a year to report that outage.

## Question



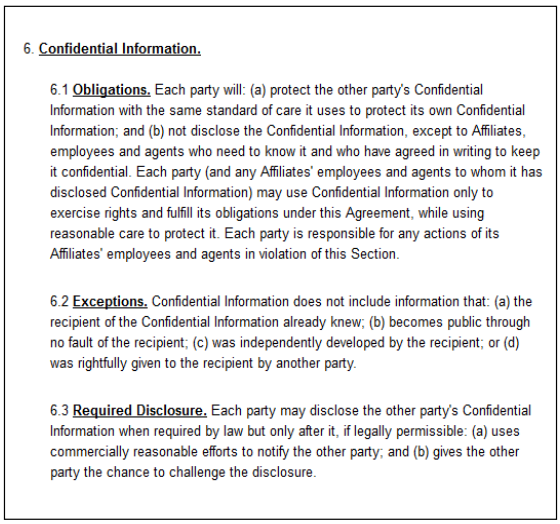

**021 And then try to obtain some sort of restitution.

So Shane we have the next question?

Shane McGraw: Yes same deal as before folks; just it is not an official polling question. But please use your Question and Answer tab there to answer: When there are proposed changes to SLAs or third-party contracts in your organization, are the operational staff promptly informed and asked for comment?

## Examples of Cloud SLAs - Google Apps

"Each party will protect the other party's confidential information with the same standard of care it uses for its own information."



6. **Confidential Information.**

6.1 **Obligations.** Each party will: (a) protect the other party's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Each party (and any Affiliates' employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under this Agreement, while using reasonable care to protect it. Each party is responsible for any actions of its Affiliates' employees and agents in violation of this Section.

6.2 **Exceptions.** Confidential Information does not include information that: (a) the recipient of the Confidential Information already knew; (b) becomes public through no fault of the recipient; (c) was independently developed by the recipient; or (d) was rightfully given to the recipient by another party.

6.3 **Required Disclosure.** Each party may disclose the other party's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other party; and (b) gives the other party the chance to challenge the disclosure.





**022 Feel free to go ahead and type away there; and we'll continue to move on.

Matt Butkovic: Sure. So another I think interesting bit of language here-- right?-- in this example: Each party will protect the other party's confidential information with the same standard of care it uses for its own information.

So we're saying here that we'll both mutually do the things we think are appropriate, as if it were our own. Right?

So I like the sentiment. But I think this is very difficult to enforce or measure against since we have no specificity.

So I think a good practice I would highlight is you should really think

about the things that are the baseline practice-wise in securing your information, your systems, your data, and how much of that you absolutely have to see reflected in the third party.

And then how you'll- what ability you'll have to know if that's really going on. You don't want it to be a black box. Right? You want to have right to audit. You want to see some sort of service auditors report- so a SOC report; right?-- to know that the things that are specified in these SLAs and in the contracts are actually being performed.

But I think John you would agree that that's, from a legal perspective, not-- this is not a legal opinion obviously. But from the- with a legal hat on that this is a very problematic description. Right?

John Haller: Sure. Sure. The basic question is: What is the standard of care? I mean, it doesn't really answer that. And as Matt alluded to, if you were to go and try to prove something based on that, that would be difficult.

And the thing that- the thing that I find interesting about this is in most cases, you know, the housing and protecting of data is a one-way relationship. Right? I mean, typically you're contracting for them to handle your data and house your data, not the other way around. It's really not a reciprocal relationship; which is

what this- what this clause actually talks about.

So it's a really good example I think.

Matt Butkovic: Yes. And I think that we've kind of become numb to contract language in our personal lives-- right?-- when it comes to cyber. Right?

So I think about- you know, I have a new iPhone and I really, really, despite all this click through of the Yes, Yes, I Agree; yes it's okay-- right?-- without that much thought about it.

John Haller: Yes.

Matt Butkovic: Because it's just kind of the Terms of Service.

But a very different situation when you're running an enterprise-- right?-- or a business where you're depending upon these things and should be pushing for more recourse than the consumer typically has.

John Haller: That's right.

Shane McGraw: So for our questions asked. We're getting a couple of replies that most organizations do not have promptly--

So what- how- what are the means to fix that? Or do you have-- is there a guideline you can suggest; or how is that corrected?

John Haller: Well I would say that if the organization is interested in improving External Dependencies Management, that goes back to that planning for it-- right?-- and talking to legal folks, talking to the contracting folks.

And from an operational perspective or the service or business owner's perspective, what cyber security concerns might they have when SLAs change? What are the things they want to know about?

And then what's the review process? What-- do we meet on this on a routine basis? When does this come up? Kind of what are the triggering events; so that if there's some contemplated change to an SLA or a contract, you let us know and we can feed back to you what the different-what the different options are and whether from a service or resilience perspective we really...

## Best Practices in Cyber SLAs

SLA management practices auditors expect to find

- "Specific and enforceable stipulations in the outsourcing agreement that activities performed by the service provider are subject to controls and audits as if they were performed by the service user itself"
- "Inclusion of provisions requiring the service provider to monitor compliance with the SLA and proactively report any incidents or failures of controls"
- "Adherence to the service user's security policies"

Source: ISACA IS Auditing Guide G4*:* Outsourcing of IS Activities to Other Organizations





**023 ...maybe need not to do that, that change to the contract.

Shane McGraw: Back to you guys.

Matt Butkovic: So I think it's an interesting data point. We've talked about sort of the limited recourse or the limited ability to influence stock contracts or SLAs.

The other side of that is your examiners, auditors, regulators and your shareholders might be expecting a high degree of control and granularity in these things.

And this is an example. On this slide you see guidance from ISACA; which is- which is an audit- it's an information systems audit organization. I'm sure most folks on the webinar are familiar with it. But this is- this is from the guide that

auditors are given for outsourcing of IT activities.

And I think the language is really interesting. So the auditors are expected to find "specific and enforceable stipulations in the outsourcing agreement." The "inclusion of provisions requiring the service provider to monitor compliance with the SLA." And "adherence to the service user's security policies."

And the third- third bullet there is really interesting. This is kind of the corollary to: We'll do the same thing we do internally-- you'll do the same thing internally we do internally, without any specificity. This is saying very specifically that the service user's security policies will be adopted and adhered to by the service provider. Right?

So you have the situation where you have low expectations and low recourse in negotiating these relationships but fairly high expectations from the folks that are examining and auditing you.

And potentially if you have some sort of breach, things that your board of directors or your shareholders may expect to find...

## Identifying Cyber Requirements

Confidentiality

- Who has authorized access?

Integrity

- Who is authorized to make changes to the data?

Availability

- When is the data needed to be accessed?





**024 ...when it examines the conditions of these contracts.

So how do we- how do we make progress? How do we improve things?

I think this slide is kind of stating the obvious; which is-- this is the classic CIA triad from Information Security: Confidentiality, Integrity and Availability.

These fundamentals apply in SLAs-- right?-- for outsourced relationships, third-party dependency management.

If you focus on requirements for the confidentiality, integrity and availability of your information and your services, you can use it as a very sound and universal starting point for developing SLAs and agreeing contracts.

So I would say back to the basics. Right? This is the blocking and tackling of information security since the dawn of time. It absolutely applies. And I think we don't often enough remind ourselves.

### Using the Service to Develop Requirements

## Using the Service to Develop Requirements

Use service requirements to develop requirements for information confidentiality and integrity

- Good:
  - Aligns with needs of the business
  - Is a check against too much investment/expense
- Bad:
  - Expensive to develop





**025 We need to boil down what we're doing into these three categories when we think about the requirements around an asset or data.

So is there a downside to all this? So if you really contemplate these relationships and you start developing these SLAs.

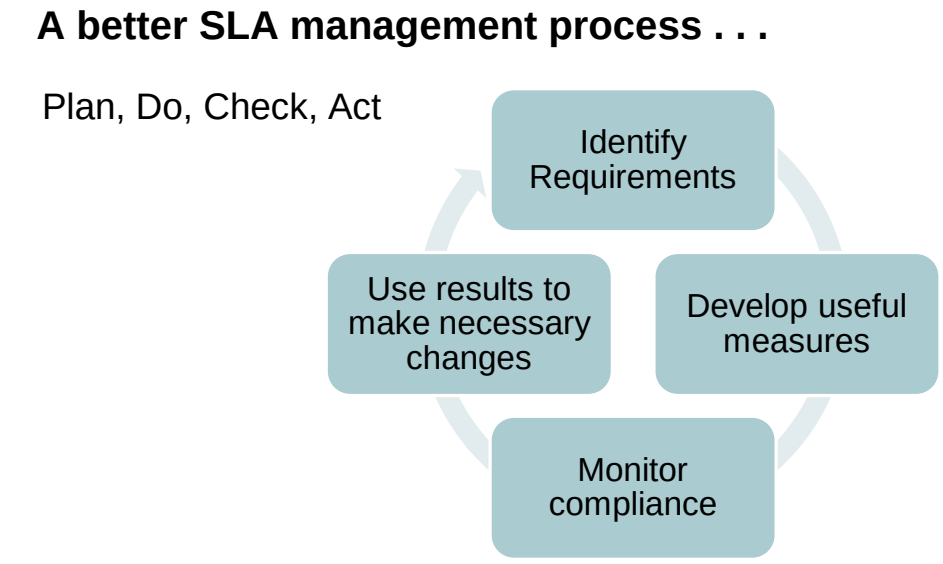
The good news is that you can then have a much better alignment between business need and the contract.

It also can be a hedge against investing too little or too much in security; because now you're making risk-based decisions.

The bad news-- and I would say that I'd probably change this slide if I had the option-- expensive to develop. Well it can be expensive to develop. But I would suggest that much of what we discussed today can be done on a whiteboard or with a sheet of paper, with just a little bit of thinking. It's not- it's not that complex an activity.

So I would say that yes, like anything else there's an investment to be made. That investment needs to be balanced against the risk. But that needs to be a conscious decision.

### A better SLA management process . . .




**026 Not simply a default setting,

if you like, in relationships with third parties.

And then an SEI presentation wouldn't be complete without a Deming cycle. I say that jokingly. I think that this absolutely applies-- right?-- the Plan, Do, Check, Act cycle is absolutely important here-- right?-- and that this really is a cycle. There's a feedback loop, and that the results should build.

### Limitations of formal agreements


**027 And that you should draw lessons learned with each iteration of the cycle.

Now John's going to give us a little more detail regarding sort of the limitations of formal agreements; and using TRANSCOM I think as an example.

John Haller: Well and, you know, we touched on that a little bit. But for instance the issue in TRANSCOM was a suspected or purported threat to the confidentiality and integrity of transportation; in this case of government assets around the world.

So I think if your- if your organization is faced with a situation like this, you absolutely- as Matt has alluded to, you absolutely need to think about SLAs and contracts. What information are you concerned with protecting with respect to the particular service; in this case transportation of assets?

But you need to keep in mind the limitations of some of those contracts. Right? If the third party-- first of all, it may be very difficult to tell if the external entity has actually breached the contract. So if you have a clause in there that says something like: The third party will report incidents that affect our information or affect a critical service; how do you prove that they didn't-- right?-- is sort of a basic question here.

If you can prove that they didn't- you know, from a legal perspective, if you can prove that they didn't, how would you ever prove damages? What is their failure to do that really worth? And what would a court actually do with that?

And of course you're going to have a contract; and the contract is very important. But I would just-- I think

the takeaway here is think through the limitations of that contract. What is that contract really getting for you? Are you sole source? Are any of these third parties or external entities sole source for your organization?

So in this case-- you know, if it's a logistics company that provides service to one part of the world-- and there's only one or two big logistics companies that may do it-- well, you know, think how- how effective is the contract going to be to actually drive their behavior? It's something to think about and to kind of--

You know, I kind of talked to- talk about it in terms of knowing your vendors, knowing their business situation and understanding again how effective this may or may not be to actually drive their behavior and provide confidence for your organization.

Matt Butkovic: But in saying all that, you're still making a risk decision. Right?

John Haller: Yes.

Matt Butkovic: But it's better to know these things and to contemplate the potential outcome than it is to just assume or blindly enter into these relationships.

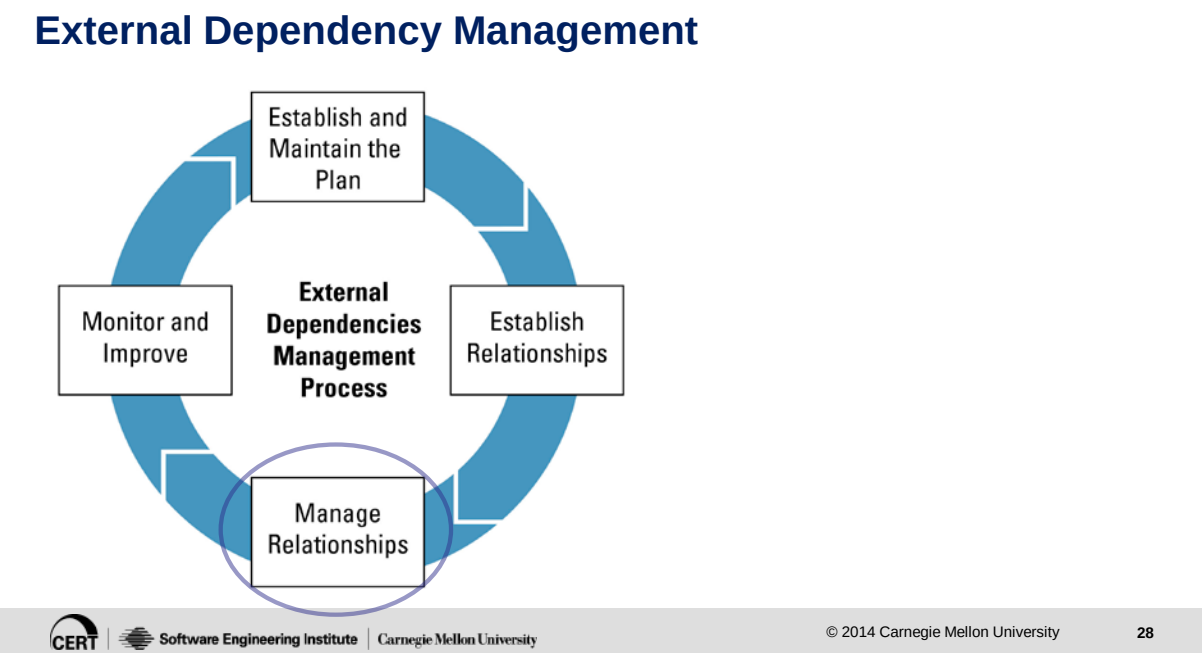
John Haller: Right, that's absolutely right. And when you say-- when Matt mentions "know these things"; even if the organization- even if you're engaging in a

relationship with a vendor or an outside party, external party, where you really don't have much opportunity to drive their behavior, you may for negotiating reasons just not be able to really enter into a firm contract to get what you really want.

It's still a very important practice to actually identify those requirements. What do we want them to be held with?

And then if we don't have- if we don't have the ability to make that actually happen, to manage that as a risk-- you know, here's an area where we've identified requirements; we may not have that in a formal contract but we can still identify it as a risk and do all the things that we do in risk management.

## External Dependency Management




**028 To try to- to try to deal with that issue.

So we're going to talk a little bit now about managing relationships.

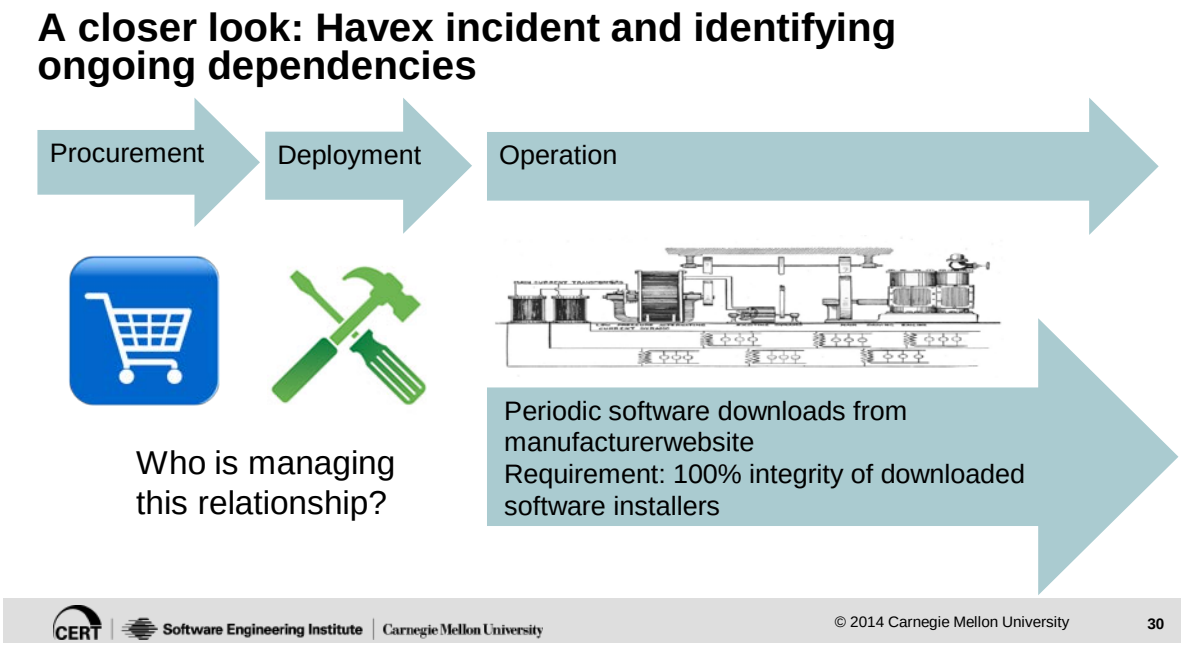
## Managing relationships: HAVEX malware / Dragonfly


CERT | Software Engineering Institute | Carnegie Mellon University © 2014 Carnegie Mellon University 29

**029 And specifically identifying dependencies and prioritizing them.

So we're going to come back to HAVEX a little bit and talk about some of the supply chain risk management implications for this- for this type of incident

## A closer look: Havex incident and identifying ongoing dependencies




**030 And how you might be able to think about this from an External Dependencies Management or supply chain view.

So in this case the electrical companies or the infrastructure providers started out-- this started out in procurement. Right?

They originally bought or procured control systems software to use in the organization. It was deployed and installed. And at that point we-from an external dependency point of view we would say that they entered into an ongoing relationship.

From that point on, the organization was getting software updates and downloads from third-party websites; and that was still an ongoing relationship that was very important to the security of those organizations.

Because obviously if there was any problem with the integrity of that software it could affect the organizations and allow- allow attackers access to the organization.

The question is: Who's managing that relationship? And it may be the case- it may be the case that it's very difficult to manage that relationship.

If it's a small provider and a very large manufacturer, maybe there really isn't that much ability to actually- to negotiate for terms; or to put a term in where, you know, if there's a problem with the manufacturer website or the installer you're notified.

In that case there are still things that the organization can do. They can do situational activities around that. They can work with their peer groups in the various information sharing agreements to make sure that they have a good awareness of any threats; and so forth.

Obviously they can look at and stay up on the alerts from ICS-CERT that are provided by the Department of Homeland Security.

Matt Butkovic: John, if I could just add to that that what you're describing are things you can do to kind of compensate. In this case...

John Haller: Yes.

Matt Butkovic: ...you don't have a choice. You've purchased this control

system. The software updates must come from that vendor. There is no alternative.

John Haller: Right.

Matt Butkovic: However-- and I'm not going to say that this would've fixed this specific situation. But if you compensate by looking at the code you're receiving, if you're looking for malware, if you do a code review, you may identify these things before they're put into the production environment.

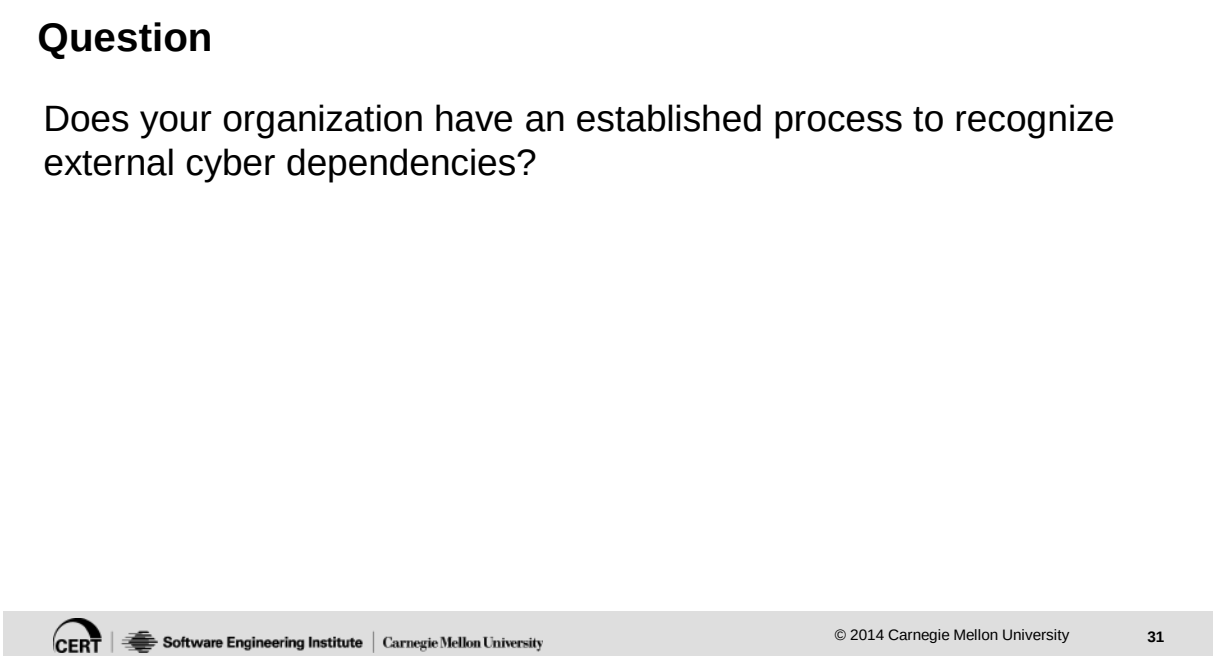
John Haller: Right.

Matt Butkovic: So there's these sort of compensating controls that can be layered in when you have these situations where you have very little ability to direct or provide subsequent feedback to the vendor, which will result in some change of behavior.

John Haller: That's right, that's right.

But the first step is understanding there's a dependency there and understanding there's an ongoing relationship.

## Question



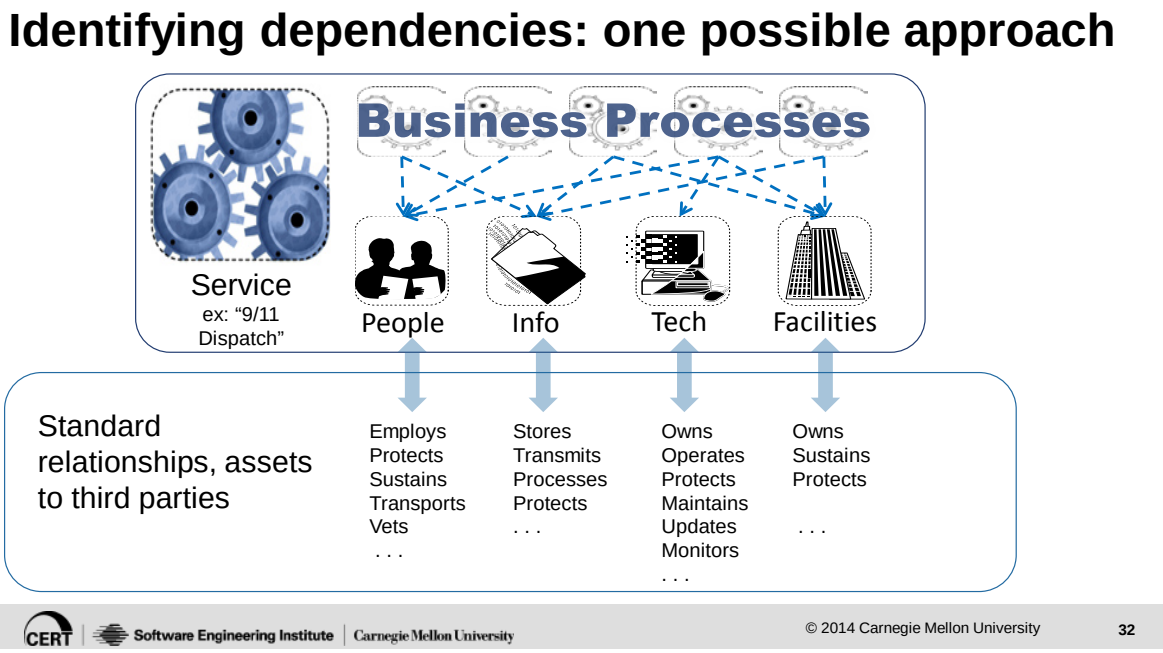

**031 And then being able to put things in place-- which Matt describes-- to help address that within the organization.

So here is another question. Feel free to jump in and type a response. Does your organization have an established process to recognize external cyber dependencies?

So we found from our research and fieldwork that just building the list, organizations just having that list of what parties they depend on, is really important; but also in many cases difficult for large organizations.

So does your organization have some sort of process, whether it's reporting from the business owners or internal auditing, to make sure that the organization knows what entities it depends on.

## Identifying dependencies: one possible approach




**032 And is managing those with a commensurate level of effort?

So go ahead; and Shane will take a look at that.

So one of the things that we've been looking at is: Is there a way to provide sort of the community or provide critical infrastructure with a better way to do this or a better way to think about this?

One of the sort of core tenets of the Resilience Management model and resilience generally is to look at assets holistically across four classes: People, information, technology and facilities.

Now I think that this is one way to think about identifying dependencies is to look at those assets-- which by the way determining what assets

support the service is really part of managing resilience or managing security-- is to look at those assets, and then try to identify: Are there third parties that have relationships with our assets or our organization?

For instance, information is kind of a fairly straightforward one, if you think about it. Are there third parties that store, transmit, process or protect our information? Or there may be other standard relationships that the third parties may have with the information asset that we rely on in our organization.

Same with facilities. Are there third parties that own, sustain or protect facilities that we use to help perform our services?

It's just another way to think about this. The example in the slide is 9-1-11 dispatch.

So if you're sitting in state and local government, and you're trying to- you're trying to protect 9-11 dispatch from a cyber security perspective, can you think about the information, which may be the numbers, the various things in your database. What third parties store, protect or transmit that for you? Can you think about the facilities and the people? And kind of think about it more holistically rather than just managing by exception or managing whenever a fire comes up.

## After identification: prioritization and tiering


**033 Or managing through some other way. It's just a way to approach it.

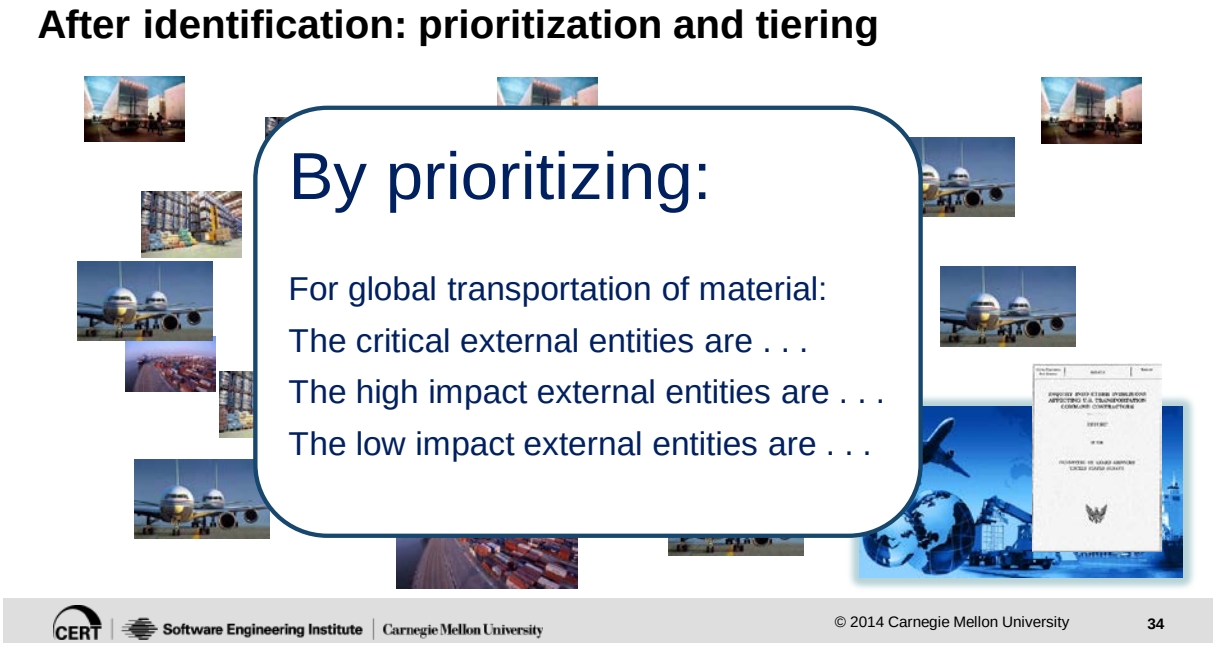
Matt Butkovic: And so I think for the sake of time John, we'll rapidly move through these slides.

John Haller: Yes.

Matt Butkovic: Regarding where to start.

So we would suggest that a great starting point is to- after you've identified your critical services...

## After identification: prioritization and tiering




**034 ...or your mission, that you associate those with assets; and you start prioritizing and tiering those relationships. So now that you understand the things that are most critical, you can identify the things that are most critical externally as well.

## Question

How does your organization prioritize vendors and other third parties for governance?

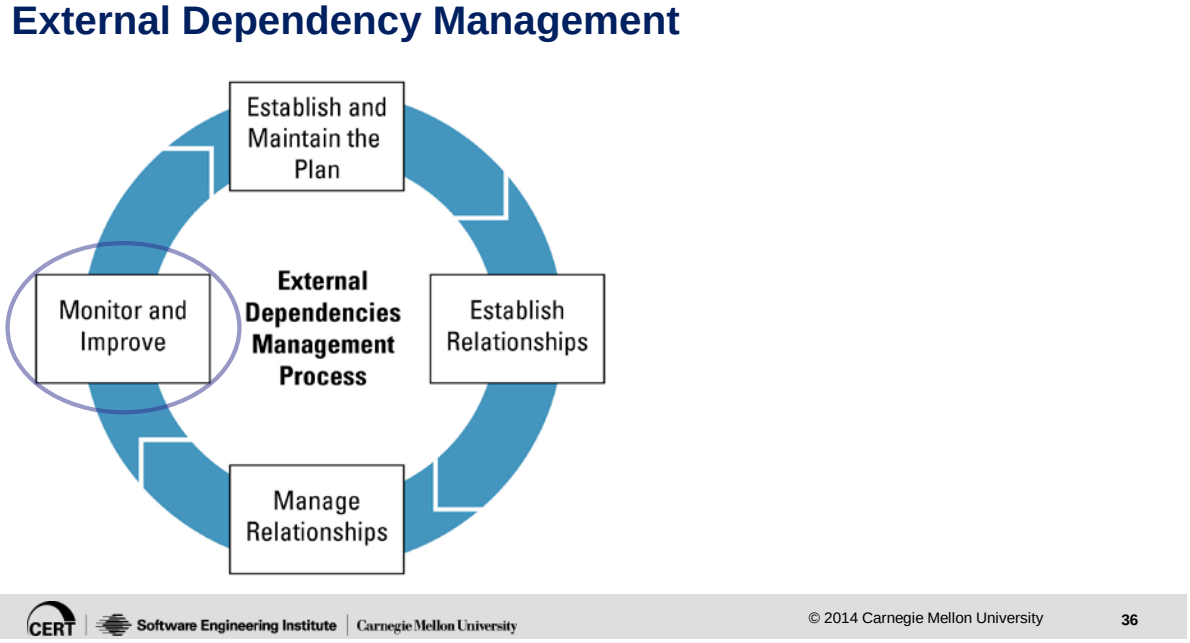


**035 John Haller: That's right, that's right.

Matt Butkovic: So John, I think again, just for the sake of time, I may sort of just move to the next portion. Right?

So let's ask the question-- the next question is: Does your organization prioritize vendors and other third parties for governance? So how do you determine which parties and relationships should be subjects to supply chain risk management activities?

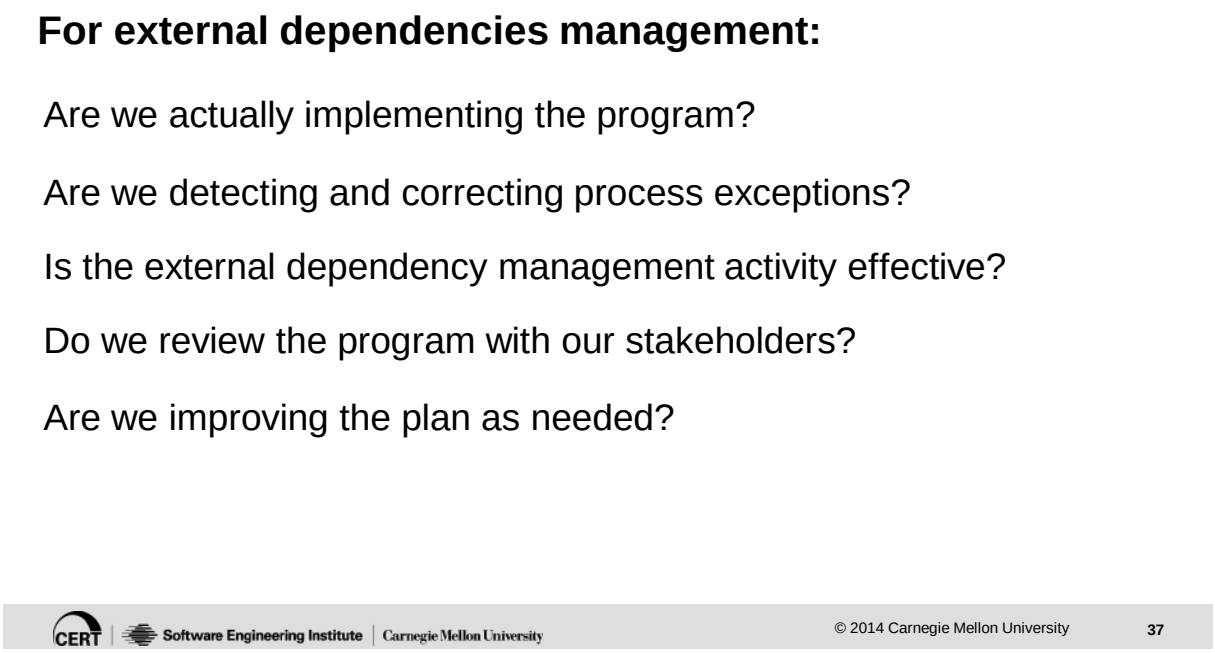
## External Dependency Management




**036 John Haller: Right. So if you have any comments or input on that, please feel free to go in.

We're going to talk a little bit about sort of managing at a higher level of maturity in organizations; monitor and improving External Dependencies Management. How do you that?

**For external dependencies management:**




**037 How do you approach that? And how can you improve how your organization does this?

So there's a few things to look at in here. Are we actually implementing an External Dependencies Management program? Are we really-- for instance if we-- in how many cases have we formed a relationship with an external entity without review or without the proper authorities? Are we detecting and correcting process exceptions?

So what this means in plain language is in the enterprise, in our organization, are people forming relationships with third parties outside the process?

And that-- for people in large organizations this probably isn't a shocker or a big surprise. Good,

aggressive people who want to do good things in your organization will form relationships with external entities without going through necessarily the right process.

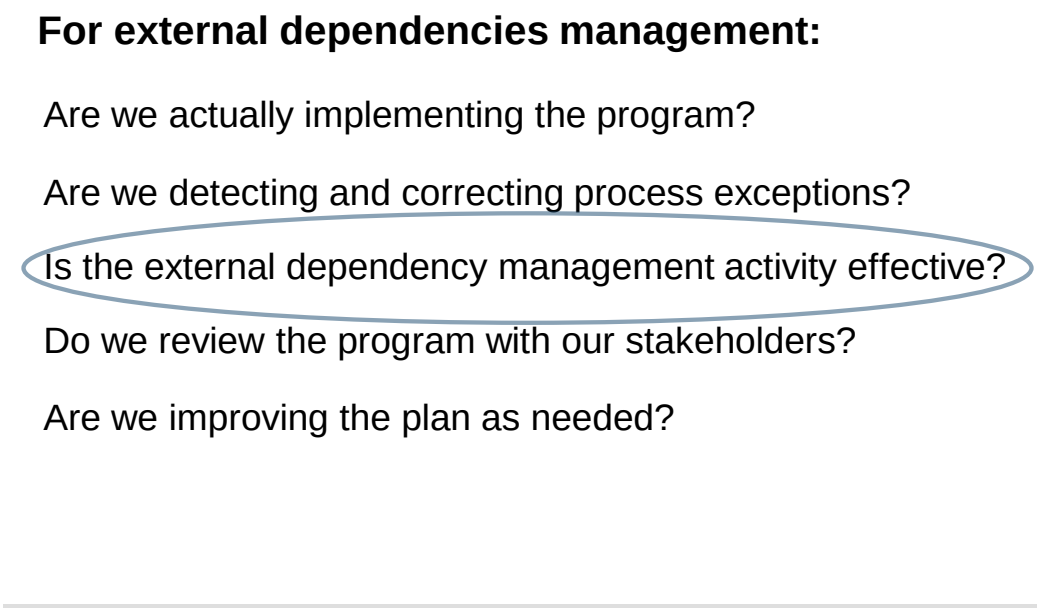
Matt Butkovic: And John we should also mention that vendors often have folks that are willing to enter into those relationships. Right? They have aggressive sales forces that look for the folks that are frustrated or are looking to kind of maneuver around.

John Haller: Absolutely.

Matt Butkovic: It may be a cumbersome internal process to procure something. And we would suggest that you need to bring those folks into the fold; that these relationships that aren't governed by these processes are not fully acknowledged or a source of danger or risk for you.

John Haller: Right. The next one is dependency management, is the activity effective? Do we review the program with our stakeholders, up to the SUS suite?

**For external dependencies management:**

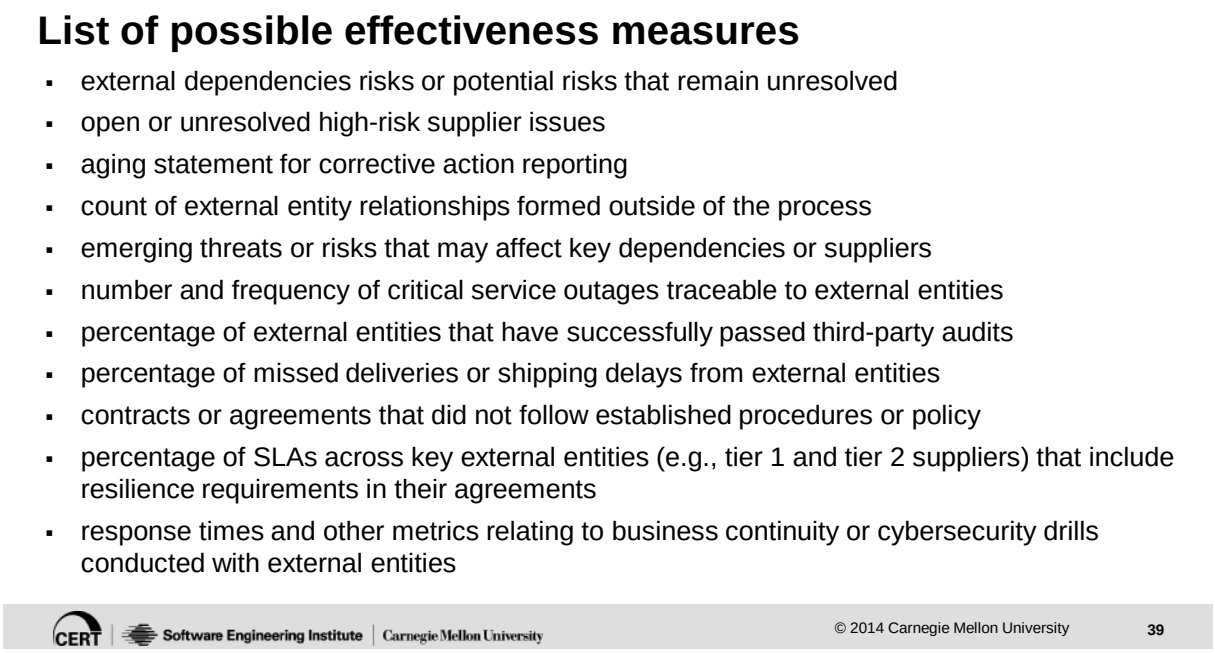







**038 And to our- to our management? And are we improving the plan as needed?

## List of possible effectiveness measures



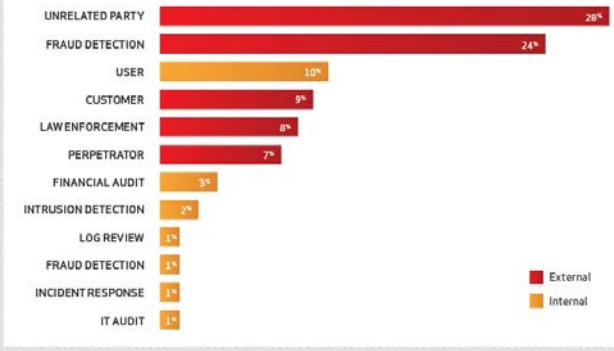

**039 So we're going to focus a little bit more on this third one: Is the dependency management activity effective?

So I'm not going to go over these in a great deal of details. They're going to-- detail. They're going to be in the slide deck for you to look at and just consider in your own context.

Matt Butkovic: John we should probably mention again the source of much of this or the bulk of it is CERT's Resilience Management Model; which you can find more information out- on, on the CERT website. So it's cert.org/resilience.

## Example area: Integrating service continuity and incident management

Figure 6: Who identifies data breaches




Many organizations devote a disproportionate amount of time and money to detection methods that fall below the 1% mark.


CERT | Software Engineering Institute | Carnegie Mellon University





**040 And also ensure that links and additional information are available as part of the package for this webinar.

John Haller: Absolutely.

Shane McGraw: Guys, just as a quick transition, we have a question that popped up a little while ago. The term 'resilience' has been brought up a couple of different times. Do you guys have a formal definition for what CERT calls resilience?

John Haller: We actually do. It's going to be in one of the slides here.

Shane McGraw: Okay.

John Haller: And it's the ability-- it's also very close to the government's definition of resilience

in the recent Cyber Security Executive Order from last year. It's the ability of the organization to sustain- to continue to provide its services in the face of disruption; I think is the short answer. But we're going to get to that.

Matt Butkovic: Yes. So just in a nutshell, there's things you can do to protect and sustain. Our view of resilience is that it is- it has both of those components; which are things you can do to proactively prevent a disruption and things you do to sustain the organization's mission or critical services when a disruption's experienced.

John Haller: Yes. We're going to look a little bit at incident management and incident reporting, from the perspective of supply chain risk management and third parties.

Verizon does a really great job with their yearly Data Breach Investigations Report; and I think this is-- this kind of sums it up.

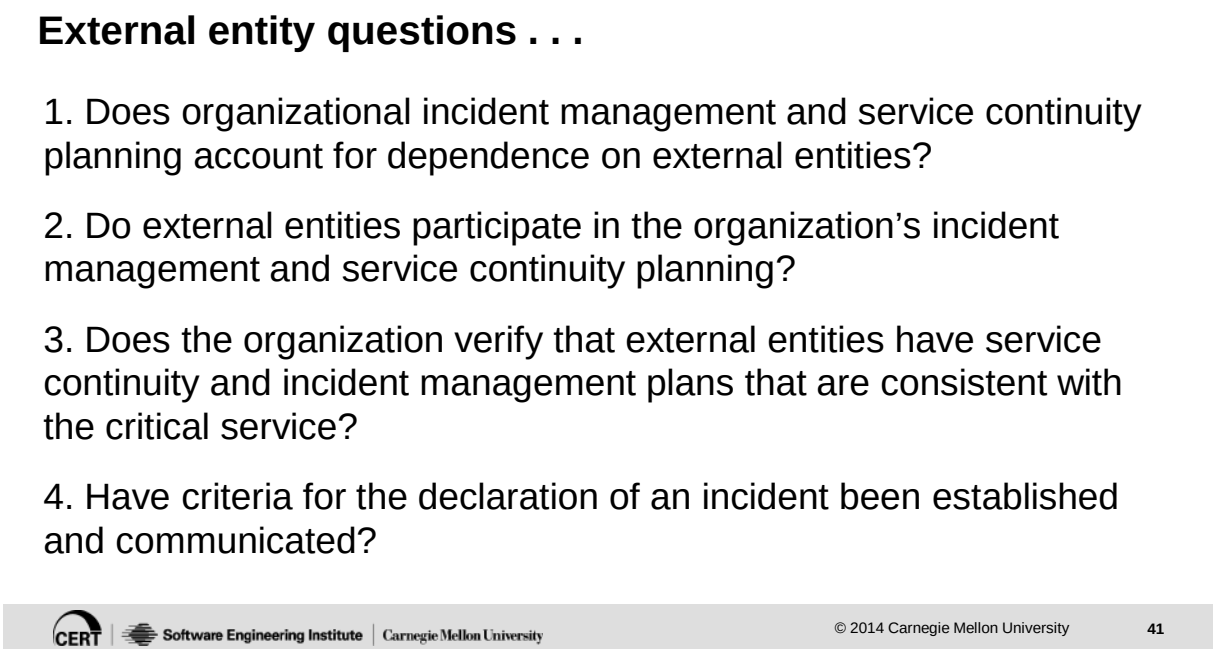
Many organizations spend a great deal of effort and money to do technical things and technical monitoring within their organization to detect incidents. That is obviously absolutely appropriate; and a requirement for managing security in many ways.

But it's very interesting that in practice in many cases organizations actually find out about the incident from a third party. It may be like a

vendor; may be law enforcement or other information sharing agreements.

But it's very interesting to me that in spite of all the great things you can do to detect incidents internally and do technical monitoring, many times it's your organization's relationships with third parties, external entities...

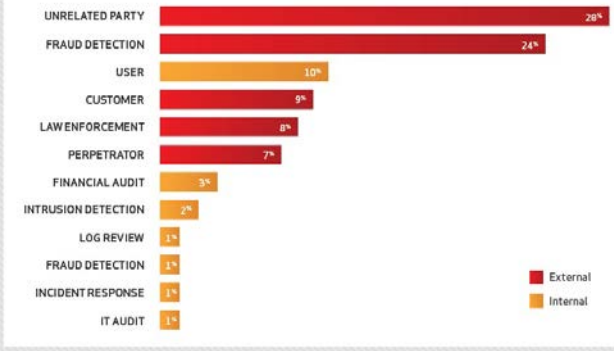
### External entity questions . . .




**041 ...including all your vendors and so forth...

## Example area: Integrating service continuity and incident management

Figure 6: Who identifies data breaches




Many organizations devote a disproportionate amount of time and money to detection methods that fall below the 1% mark.


CERT | Software Engineering Institute | Carnegie Mellon University



40

**040 ...that will allow you to become aware of incidents that may affect the organization.

Matt Butkovic: Sorry John, if we could just go back for a just a second.

John Haller: Yes.

Matt Butkovic: Please. And this is a really shocking chart when you think about it.

John Haller: Yes, yes.

Matt Butkovic: So you're saying that the third party that's had the breach is notifying that they've had a breach. We're saying-- unrelated third parties I see.

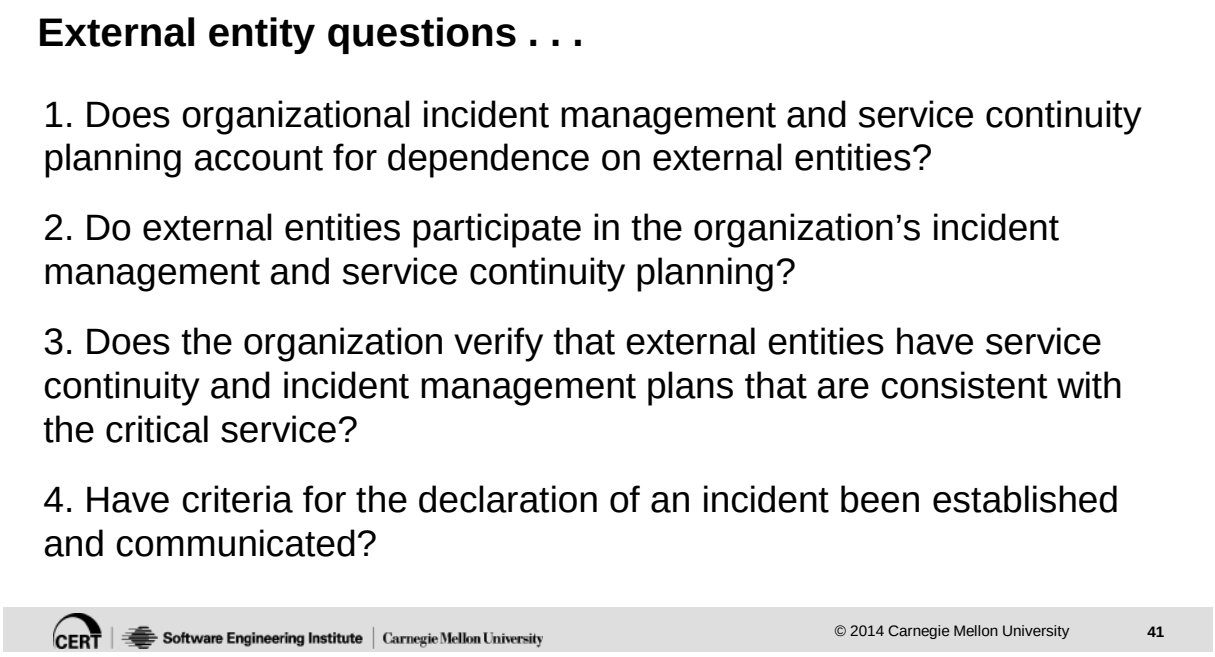
John Haller: Absolutely.

Matt Butkovic: And so what I find really disturbing is that customers are far more effective-- as a former IT auditor-- than IT Audit is; or that intrusion detection systems aren't identifying these things.

So I think depending on your customers and unrelated third parties as a detective control to let you know you've been breached is a really scary proposition.

John Haller: It is a scary proposition, absolutely. But I think that it's important for organizations to realize that in many cases this is what's going to happen.

### External entity questions . . .




**041 And to sort of put that in their tool bag; and to build those relationships with third parties so that they can become aware of them.

But absolutely. I think it is a shocker, yes.

So these are sort of a snapshot of external entity questions; things you might want to think about when you're- when you're talking service continuity and incident management with a third party.

Do they have- or does your own- do your own plans and do your own processes account for dependence on a third party?

That may be as simple as: Okay if we have a service continuity plan and we reply on a third party, is the point of contact information and telephone numbers and email addresses, is that updated, so we can reach the right- the right people, if and when there's a disruption?

In many cases it may be important for the vendors or external entities to participate in your service continuity and incident management planning; for them to be part of that. And also for you to test with those third parties.

Matt Butkovic: So exercises John.

John Haller: Exercises; absolutely right.

Does your organization verify that- do you verify that they have incident management plans or BCDR service continuity plans that support your organization and your critical services?

And the last one is something we're going to go into a little bit more in depth here. Are there criteria for the incidents that you want to know about in your third parties? And have you communicated those?

### Incident declaration criteria:

## Incident declaration criteria:

Report incidents that "affect organizational information resident or in transit on vendor systems"

How do we assess the effectiveness of this control?

Very challenging, some possibilities:

- Event reporting?
- Reporting on technical detection?
- Situational awareness and collaboration?






**042 And are you monitoring those to make sure that they're actually being acted upon and that they- that they are supporting you?

So we'll go into a brief example here. So this is- this criteria listed on the first line is very similar to the criteria in this actual incident, that appeared in some of the external entity contracts. And it was a requirement to report incidents that affect organizational information resident or in transit on vendor systems.

So the question is: How do we monitor- how do we know that's effective; and how do we monitor that as an ongoing proposition, to know that okay we have this in our contract but are they actually doing this? How are they doing it? Are they doing it in a timely way?

Well so there's a few ways to approach this. The first way probably is, back to a previous slide: Have you prioritized those external entities so that you can put time and money into managing that relationship with the right entities?

And it kind of goes back to the old maxim: If you defend-- maxim-- if you defend everything you defend nothing. Right? You have to do some prioritization and tiering so that when you are managing this relationship in an ongoing way you're doing it in an explainable, efficient way.

Matt Butkovic: There has to be criteria. So there has to be some idea of magnitude or materiality of the incident; otherwise you could- you can drown in the information essentially.

John Haller: That's absolutely right.

So what are some ways to get it? It's a challenging area. And I think there's actually a question coming up here for the audience. But would you look at event reporting? Whether it's in the SLA or contract or not, would you want them to tell

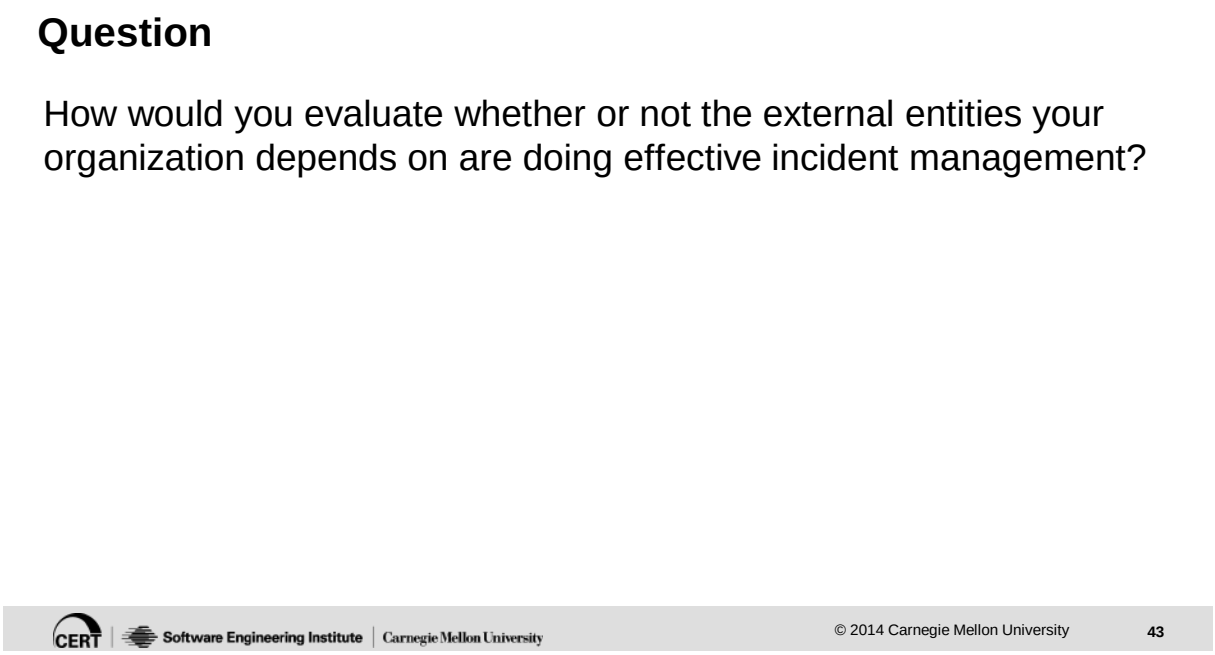
about- tell you about the security events; something that is not quite as important as an incident but may still sort of be a precursor?

Would you want to know about what they're doing from a technical perspective in their environment? I think that's kind of a very straightforward sort of obvious one.

The other thing is if you understand the vendors and third parties, can you collaborate with them or can you collaborate with peers so that you have some situational awareness over the threat environment and what those third parties may be exposed to?

And I think the- you know, I think the takeaway here is in many cases there's no substitute for service reviews and actually working closely with the third party; and for the third parties, the external entities, that are truly critical, actually being there and communicating on a regular basis.

## Question




**043 To have awareness of what's going on. I mean, that's-- I think that's a great takeaway from this.

So here's a question for the audience: How would you evaluate whether or not the external entities your organization depends on are doing effective incident management in support of your organization?

## Conclusion – a resilience approach


**044 So feel free to put a comment in there. We'd be happy to chat about it.

So we're going to conclude here in a little bit. We're going to talk about a resilience approach.

## Cyber Resilience Value Proposition

**Resilience management** provides support to *simplify* the management of complex cybersecurity challenges.

**Efficiency:** not too much and not too little; resilience equilibrium

- balancing risk and cost
- getting the most bang for your buck
- achieving compliance as a by-product of resilience management

**Roadmap:** what to do to manage cybersecurity; flexibility and scalability

- using an overarching approach - which standard is best
- deciding what versus how to manage cybersecurity risk

**Cybersecurity ecosystem:** addressing the interconnectedness challenge

- managing dependencies
- addressing both internal and external organizational challenges and silos





**045 And some ways that your organization kind of can think about this from a fairly broad perspective.

So the- so CERT and the SEI have a number of tools that are out there to help you- to help organizations look at this from sort of a more holistic perspective. And really it goes back to the previous slide.

This is a complex area; and one of the best ways to tackle it is to look at this from a holistic perspective and to look at it across your organization. That's a way-- some of those basic activities like identifying and prioritizing services, figuring out what are the core assets that really support those services?

That's something that-- it needs to be done and managed and improved over time. But it's something that

you do and can help your organization with a variety of cyber security problems or cyber security goals. And that ranges from external dependency management to insider threat.

Okay if we're worried about insider threat, what are the- what are the- what are the crown jewels that we really need to protect and have good controls on; to a variety of different areas.

So that's kind of what we mean by the value proposition here. Not too much and not too little. Getting the most bang for your buck.

And also if you're- if you're thinking about compliance and you have a lot of compliance obligations, incorporating that into your management so that you can have that as a byproduct of resilience management; and be able to answer some of those- some of those requirements as well.

Matt, any comment on that?

Matt Butkovic: So John I think you've hit on the head; which is that we're suggesting that if you take a resilience approach, you ultimately simplify a complex situation.

## Process Maturity for Cyber Resilience

The degree of process maturity can help to answer several important questions when managing cyber resilience:

- How well are we performing today?
- Can we repeat our successes?
- Do we consistently produce expected results?
- Can we adapt seamlessly to changing risk environments?
- Are our processes stable enough to depend on them during times of stress?
- Can we predict how we will perform during times of stress?

**Process maturity helps avoid the pitfalls of a project (set and forget) approach to cyber resilience and helps "make it stick."**





**046 John Haller: That's right.

Matt Butkovic: And then have more granularity in the control you can apply to these relationships.

John Haller: Yes. So another sort of key component of this-- and this frankly goes back to the diagram that we've already talked about-- is process maturity for cyber resilience.

You know, it's-- I think the line on the bottom is really kind of the important part here. Cyber security is not a project. Right? An improvement effort is not a-- you know, I do this, I put some things in place and then I set it and forget it; obviously. Right?

The question that- type of questions that organizations should be concerned with are: Can we repeat

this, can we sustain this? When things change-- because they will, like tomorrow-- can we actually continue to have a certain level of cyber security?

One of the things that we kind of always- we kind of always use when we talk about resilience is: Can we predict how we will perform in times of stress?

Well I think it's kind of important to remember that stress doesn't just mean an incident or, you know, a information breach or something like that; or, you know, God forbid, a disaster at some point. Stress can also mean organizational stress. Right?

From the perspective of procurement and managing relationships, what happens when there's a reorg within the organization? What happens when there's a merger? I mean, are there--

Matt Butkovic: Sorry John. If someone leaves the organization.

John Haller: Absolutely.

Matt Butkovic: That has a deep knowledge of that relationship, is an example.

John Haller: That's right.

Matt Butkovic: Of a stress that's sort of more routine or mundane. This is not, you know, only hurricanes and nation state level

cyber attacks. It's the everyday sort of complications and disruptions you face as an organization.

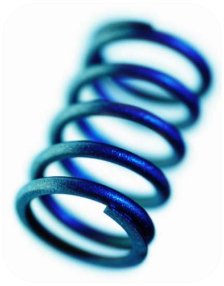
John Haller: Right. You don't want to be in a position where essentially Matt is your embodiment of relationship management and knows everything about SLAs. I mean, there needs to be something in place so that that can be sustained over time; at least for the very critical things your organization does.

Matt Butkovic: Yes John. I would just-- just at a high level, for the sake of time. The CERT Resilience Management Model is a capability maturity model; which means it addresses, as you're suggesting, the institutionalization, the enduring nature of the processes in the organization. And this is a tie back to the CMMI.

## What Is Cyber Resilience?

*"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"*

- Presidential Policy Directive – PPD 21
February 12, 2013



| Protect (Security) | Sustain (Continuity) |
|---|---|
| Perform (Capability) | Repeat (Maturity) |





**047 And the view of capability maturity that the SEI has been- has been offering for a long time to the software community.

John Haller: Yes. So the question was asked previously-- this is a great question: What is cyber resilience?

This is actually the definition from the Presidential Policy Directive, PPD 21 that was put out last year: The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. It includes the ability to withstand and recover from deliberate attacks, accidents or naturally occurring threats or incidents.

I think one of the basic things behind resilience is it's very important to think about threat and what may- what your organization may

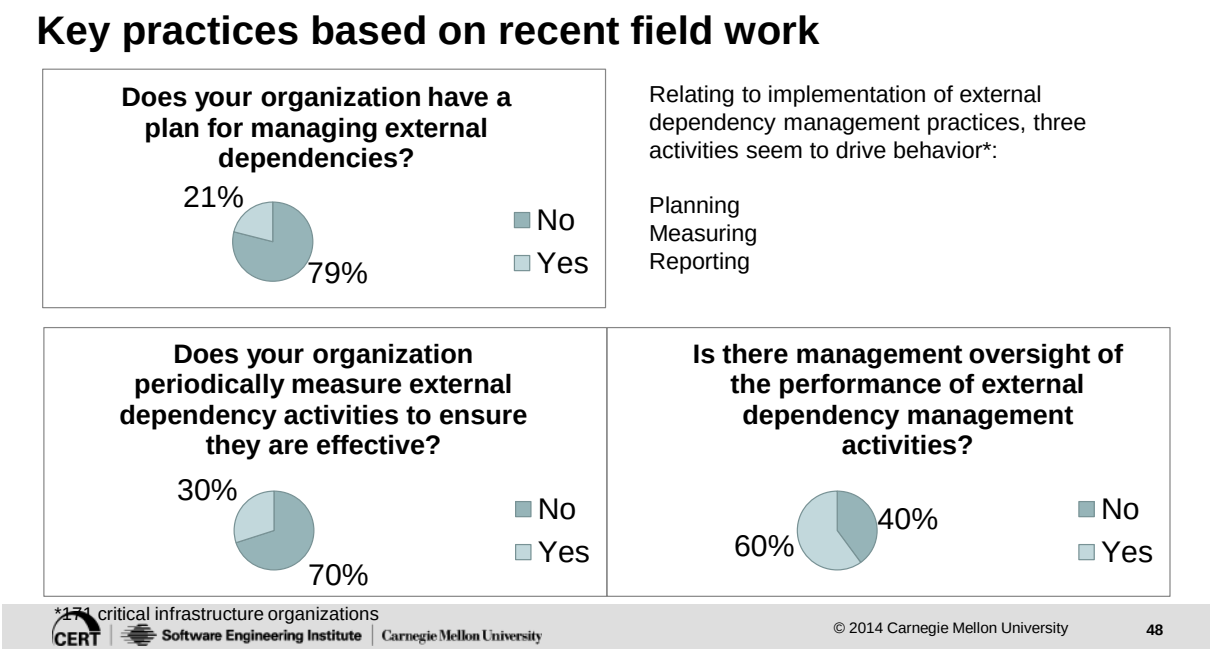
experience. But it's also very hard to predict what those threats will be.

So to the extent that you can put processes and capability in place that really are sustainable, that really are prepare the- that really can prepare the organization for that- for those types of disruptions, whatever may come, you'll benefit.

Matt Butkovic: So John just to add onto that; that we're suggesting that managing the consequences side of the equation risk-wise is very important. That with a long enough timeline the odds of something bad happening are really pretty much-- it's certain that you'll have something bad happen within the organization.

So focusing on threat is really important.

## Key practices based on recent field work




**048 But focusing on managing the consequences of some sort of detrimental impact is equally important.

John Haller: Right. So we'd kind of like to close, or come close to closing I suppose, with a little research that we've done based on some recent fieldwork.

So what we've done, as Matt alluded to, is we've-- as part of an assessment activity that we've done with critical infrastructure, specifically around 170 critical infrastructure organizations, we've gathered information about what they do to manage external dependency risk.

Specifically we're looking at what key practices correlate to implementation?

And I think that's kind of important. Because we're not saying- we're not really looking at effectiveness. It's kind of difficult and a different project to say that these specific things were effective.

But when we-- when you look at this chart, this means that certain practices result in more implementation within an organization of practices around external dependency risk; practices like putting the cyber security requirements in SLAs, monitoring third party performance, prioritizing external dependencies and so forth.

So what this research says-- and it's a relatively small sample size. I think we're just at the first start of really being able to say things in a broader way. But what this research says is that with- in relation to implementing External Dependencies Management, there are three high level activities: Planning, measuring and reporting. Right?

So if you're planning around this, if you're trying to measure implementation and effectiveness, and if you're reporting to senior management, the organization- organizations generally have a lot more in place, a lot more of the right practices in place, to manage external dependency risk.

And these are some of the-- based on sort of a, as Matt alluded to, sort of a mixed bag of critical

infrastructure organizations. These are some of the results.

Seventy-nine percent of organizations we looked at do not have a plan for managing external dependencies.

Seventy percent of them do not really measure the activity.

And 40 percent of them do not report and engage in higher level management oversight of the activity.

Matt Butkovic: It's kind of an interesting disconnect in the data-- right?-- that you can see that the practice level, the things we're saying are important-- right?-- are generally not being done. But there is oversight.

John Haller: Right.

Matt Butkovic: So I guess things like today's webinar I would hope-- right?-- and the CERT Resilience Management model can help improve the way that folks are managing this.

## External Dependency Management – Work Underway at Carnegie Mellon CERT

Two key components:

1. An organizational assessment for external dependencies management
2. Exploring better ways for organizations to identify and prioritize cyber dependencies

*"The Information and Communications Technology (ICT) services used by operators of critical infrastructure, on which the delivery of a critical infrastructure service depends."*





**049 John Haller: That's right.

Matt Butkovic: If they are doing oversight, you'd hope that oversight's improving.

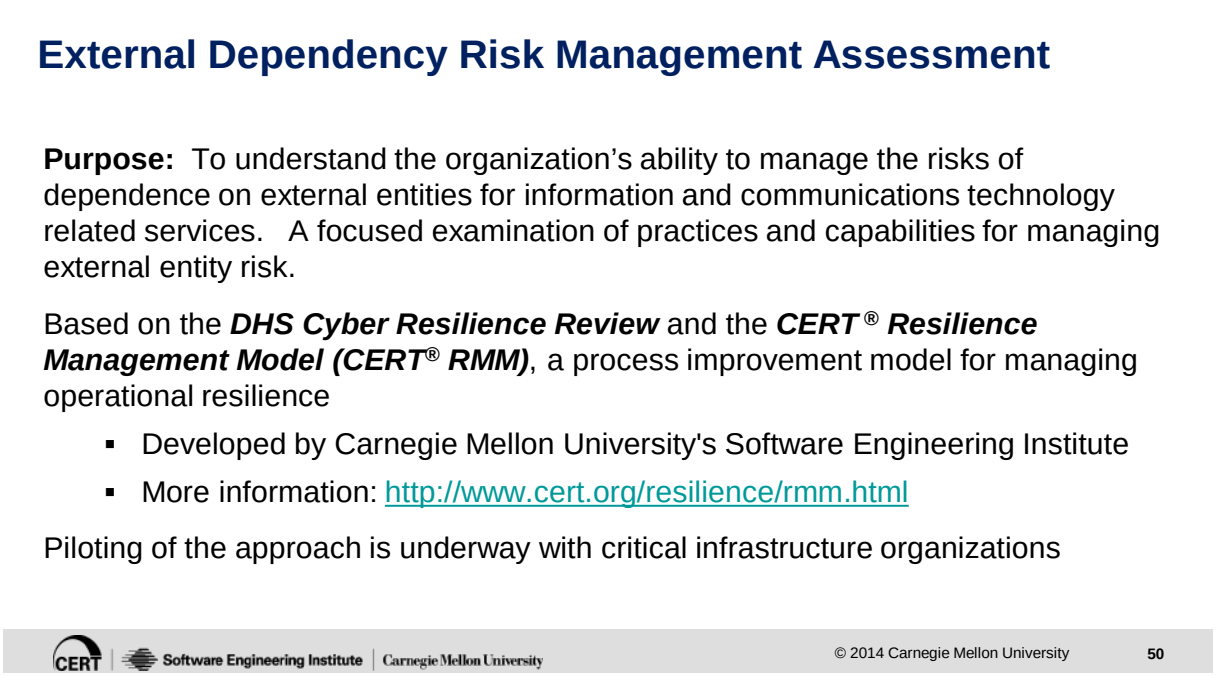
John Haller: Right. So I'm going to talk next about a few things we're working on here. One-- these are both in connection with some of the government sponsored work that we do.

The first one is an organizational assessment for external dependencies management. This is a three-hour- three-and-a-half hour assessment that we're currently developing to help to go into more depth in this area, and to help organizations understand how well they're managing external dependencies now; across some of these domains, from- all the way

from managing relationships initially. I mean-- I'm sorry-- forming relationships initially to managing them in an ongoing fashion, all the way through to thinking about external entities from the perspective of service continuity and incident management.

And we're in the early stages of the second one; which is really--

### External Dependency Risk Management Assessment




**050 Can we provide better ways for organizations to identify and prioritize external dependencies?

So this is a little bit more depth on the external dependency risk management- external dependency management assessment. This is based on the Cyber Resilience Reviews and on the CERT RMM, the Resilience Management Model.

If you have- if your organization has an interest in a three- in a three-and-a-half-hour assessment--

Matt Butkovic: Facilitated assessment.

John Haller: Facilitated assessment-- thank you. We will actually come onsite to your organization, sit down-- and this is fully funded. We will actually come onsite, sit down with your organization and look in depth at how the organization is managing external dependencies over time; and then feed back a report that provides some sort of recommendations and options for consideration where the organization is strong and weak. Please contact us.

Matt Butkovic: John I just wanted to mention-- as well I know I kind of pressed for time-- but there's also an effort to align the criteria of the NIST Cyber Security Framework, the NIST CSF, with the Cyber Resilience Review, the CERT RMM, and also with these kind of nascent emerging supply and chain risk management assessments.

John Haller: That's right.

Shane McGraw: Is it safe to say that the RMM is the "what" people need to look for in some of these assessments; or the "how"?

John Haller: Well the-- cyber resilience review and any of these assessments are still approaching or

still looking at the "what". Right? Because we're still looking at the goal level: What should the organization be thinking about and doing; and then down to more specifics, sort of touching on "how".

But one of the strengths of RMM or the Cyber Resilience Review or the External Dependencies Management assessment is it is really focusing on the "what". Right?

Shane McGraw: Mm-hm.

John Haller: It's focusing on a way for organizations to understand their capability internally; and hopefully in the future more to compare themselves against other organizations.

That's a strength because not all of the sort of very specific things are going to apply to every organization. So it is a little bit higher level. I think Matt-- any comments on that Matt?

Matt Butkovic: Yes I think Shane I would describe it this way; that the CERT Resilience Management Model gives us sort of a body of knowledge, a body of practices that are then sort of applied in different forms, the Cyber Resilience Review being one them, the External Dependencies Management assessment being sort of a derivation of that.

So as John said, I think it's still the- it's still the what; although the how is suggested.

## In Closing…….

- External dependency management is one of today's key business challenges
- Dependencies extend well beyond just your vendors
- Relationships and partnerships are key – organizations cannot effectively manage dependency risks on their own
- The complexities of the today's cyber and physical disruption landscape requires new tools
- Taking a converged approach to the challenge is key
- Resilience management can help provide a roadmap to simplify the management of operational and dependency risks



**051 And it's not unlike the NIST Cyber Security Framework in that regard.

Shane McGraw: Okay.

John Haller: So in closing-- and I think we've covered a lot of ground here-- I think one of the big things is dependencies extend beyond only your vendors. Right?

You need to think about this holistically. It may be organizations that you-- like for instance government organizations, transportation networks, other types of external entities that you rely on to support some of your cyber services, that you should really think about and think about it holistically.

Partnerships and relationships are key. Right? If you think about

situations where frankly you may not have that ability always to negotiate a firm contract with a third party, and you may not be able to drive their behavior. Right?

Well one of the ways to mitigate that is to talk to your industry peers, to exchange information in targeted, prioritized ways. Right? Not to subject yourself to an information overflow. But to think about what you can do to mitigate some of those risks and put some compensating controls in, in that area.

New tools and new ways of looking at things. And I think one of the takeaways is that there is- there's a need out there for ways to- for organizations to judge their capability and be able to do this better.

And I think that resilience- the Resilience Management Model and the resilience approach provides a lot of value here and can help the organization think about efficient ways to manage this type of risk and to gain some efficiencies from it.

We're not suggesting necessarily more effort, more expenditure. We're suggesting the right amount of effort and smart ways to manage some of that.

Matt Butkovic: Optimizing it John, I think is one of the key--

John Haller: Optimizing it

## CMU – CERT Supply Chain Risk Management Symposium , January 15th 2015 in the DC area.


**CMU – CERT *Supply Chain Risk Management Symposium*, January 15th 2015 in the DC area. For information contact info@sei.cmu.edu**

**Contact Information:**
**John Haller – jhaller@cert.org**
**Matthew Butkovic – mjb101@cert.org**





**052 Yes that's absolutely right.
So.

That-- I think Shane the windows are still open, if anyone has any questions.

In the materials there's going to be-- there are-- our email address is in here. So you can certainly contact us.

And also there's a note in here with respect to the Supply Chain and Risk Management Symposium that we will be holding on January 15th in the DC area. We'd love to see anyone who's interested there.

Matt Butkovic: Sorry John.

John Haller: You have a question?

Matt Butkovic: Yes. A thought about the symposium is that the audience-- there is-- it's kind of a closed event. Right? So we only have so many seats available. So if you're interested, we'd love to hear from you and guarantee you a spot in that symposium.

John Haller: That's right, absolutely. That's right.

Shane McGraw: Okay. So the queue is open for questions. We have a couple in.

I just wanted to give two good examples of some comments that came in from the questions we posed throughout the event; and just let you reply. They seem like they were spot on.

But one from Neil saying: We have a tiered vendor mechanism, depending upon criticality of services.

So like you said, you can't protect everything.

John Haller: Right.

Shane McGraw: So pick the ones that you--

John Haller: That's absolutely right, yes.

Shane McGraw: And also from Denise another: We have a triage process for new third party relationships and a review process for established relationships.

Matt Butkovic: That's great; I mean--

John Haller: It's important.

Matt Butkovic: That's very encouraging to hear.

John Haller: Right.

Shane McGraw: Okay. So let's get into some questions. Folks feel free to type them in, in you have them.

From Don asking: Can an SLA on cyber security transfer the cost of a cyber incident to the third party vendor?

John Haller: I think that's a really good question.

I-- my opinion is that is very difficult. It's difficult because-- you know, it depends on the negotiating ability and the positioning of your organization. Right?

I mean, generally the legal system takes a pretty broad view of contracts. If you can get them to agree with it, and it's not an unconscionable contract, the legal system will support it.

But I'd say it's very difficult. You know, in cases where you can clearly define breach-- what does breach mean?-- and in cases where you can clearly define what are the damages, then maybe.

However even doing that, you know, really relies on a lot of internal processes at your organization. First of all, to understand what it would actually cost. Right? And that's very hard to predict.

So it's difficult. It's certainly- it's certainly not impossible; but it's very difficult to do that.

Matt Butkovic: So just to add onto it John. I think that one of the things that needs to be part of that discussions thinking about the cost of things that aren't as readily visible.

John Haller: Yes.

Matt Butkovic: So think about reputation damage. Think about a drop in your stock price. Think about things that-- you know, they're certainly tangible but it's kind of viewed as intangibles. Right?

How do you-- if you have a breach that has a devastating consequence on the brand image of something in your organization, I don't think you're likely to be- to seek restitution really sufficient to cover those losses.

John Haller: Yes there are- there are examples of contracts in other spaces that have nothing to with cyber really where-- you know, the contracting party had a lot of negotiating ability and they could get a third party to agree, for instance, to liquidated damages; and the liquidated damages were so severe that-- absolutely, you know, if breach

is defined clearly, you know, and there's a breach, they're going to get paid. Right?

But that's really difficult to do in this space. You know? Also for many of the reasons that Matt mentioned. It's hard to know what the costs are. And I think it's just not- not-- the tools used are sort of immature, in my opinion, with respect to cyber security.

Matt Butkovic: Yes I think adding to that challenge is that the cyber security insurance market is still sort of formative and a bit immature. Right?

John Haller: Right.

Matt Butkovic: Meaning that you can't always find protection that would be equivalent to some physical protection you'd find; for instance, you insure the factory in case it burns down. It's hard to find an equivalent level of coverage in cyber often.

John Haller: Yes. So try to do it that-- you know, count on some of your internal processes; you know, in case it fails.

Shane McGraw: Good. Just two more quick questions in the queue.

This from Neil asking basically can we define resiliency as the business continuity or disaster recovery? Is that--

Matt Butkovic: No I think--

Shane McGraw: Not cool to say or-

Matt Butkovic: I think it's one part of the equation. And I think this is a really good question. We get this a lot.

John Haller: Yes.

Matt Butkovic: We're suggesting-- Neil, what we mean by resilience is not only the things you do to sustain your operations when something disruptive happens-- that's traditionally business continuity and disaster recovery-- but also things you can do proactively to protect and to the best extent possible mitigate the conditions that lead to those disruptive events. So it's two parts to the equation.

So I would say yes it encompasses that; but it's not exclusively disaster recovery or business continuity planning.

John Haller: Yes, yes.

Shane McGraw: And this is the last one in the queue. So if you have one, we have a couple of minutes to type them in. Otherwise we'll finish up on this.

John mentions- you mentioned the symposium a couple of times. What's the profile of the person you're looking to attend this? What's the profile of who should be attending?

John Haller: Okay that's a really good question. So we're looking both

for folks who are I would say fairly executive level and responsible for overseeing this in your organization.

But also we're looking for folks that are-- especially in the afternoon section of the symposium-- we're looking for folks that are dealing with this on a regular basis; in other words who have to figure out-- you know, if you're someone who has to figure out what are your organization's dependencies and how do I go about allocating resources to actually handle those-- you know?-- or put additional staff time or money into managing relationships? The afternoon section is going to look at that a little bit more.

So I would-- please send me an email and I'll get the flyer and so forth out to you.

But we're looking at government sector or kind of DoD focused and private sector. And our basic idea is that the public and private sectors, they're-- they face similar problems. There's more about this problem that is alike than different between those two sectors. And that's what we're really going to explore.

But in the afternoon we definitely want to kind of look at the daily business operational way that this is being done; and how it can be done better.

Matt Butkovic: So both practitioners and also executives, both from the DoD or federal civilian

agencies; and also from private industry. It's a pretty wide cross-section of folks we'd like to participate in this symposium.

John Haller: Absolutely. Yes and if there's questions, email me and we'll talk on the phone; I mean, you know, absolutely.

Shane McGraw: Great. John, Matt, thank you for your presentation.

Matt Butkovic: Thank you.

Shane McGraw: Terrific. Again thank you for everyone attending.

We do request that you fill out the survey upon exiting as your feedback is always greatly appreciated.

And don't forget the Materials tab, to walk away with various PDFs from CERT work in the area of resilience management.

And lastly we hope you join us next week for the next SEI webinar; and it'll be Risk Probability Number, by Will Hayes and Julie Cohen.

Have a great day everyone. Thank you.

John Haller: Thank you.