# Evolving Role of the Chief Risk Officer

## Table of Contents

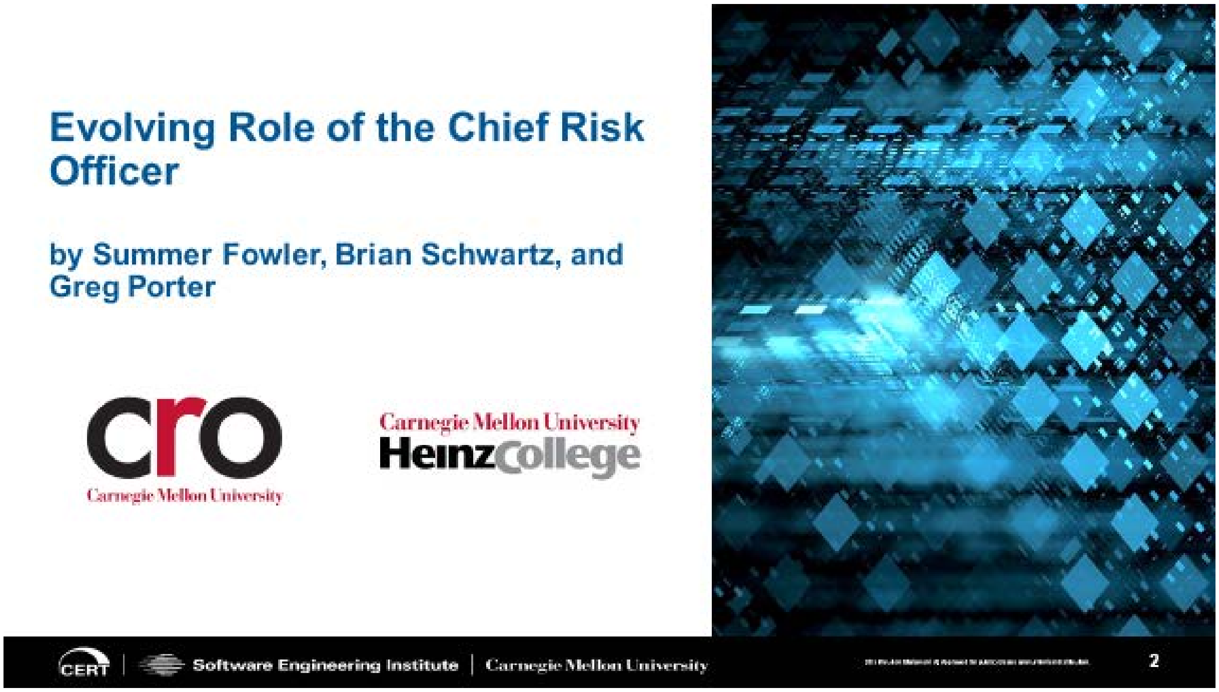
## SEI WEBINAR SERIES | Keeping you informed of the latest solutions

SEI WEBINAR SERIES | Keeping you informed of the latest solutions

#SEIwebinar

Software Engineering Institute | Carnegie Mellon University

## Evolving Role of the Chief Risk Officer



Evolving Role of the Chief Risk Officer

by Summer Fowler, Brian Schwartz, and Greg Porter

cro Carnegie Mellon University

Carnegie Mellon University Heinz College

CERT | Software Engineering Institute | Carnegie Mellon University

2

**002 Presenter: And hello from the campus of Carnegie Mellon University in Pittsburgh, Pennsylvania. We welcome you to the Software Engineering Institute's webinar series. Our presentation for today is the Evolving Role of the Chief Risk Officer.

Depending on your location, we wish you a good morning, a good afternoon, or a good evening. My name is Shane McGraw, your moderator for the presentation. And I'd like to thank you for attending.

We want to make today as interactive as possible. We will address questions at the end of the presentation. You can submit those questions to our event staff at any time using the questions or the chat tabs on your webinar control panel.

Another three tabs I'd like to point out are the download materials, Twitter, and survey tabs. The download materials tab has a PDF copy of the presentation slides there now, along with an overview of our CRO program. The survey we ask you to fill out upon exiting today's webinar, as your feedback is always greatly appreciated. For those of you using Twitter, be sure to follow @CERT_division and use the hashtag #seiwebinar.

Now, I'd like to introduce our talk facilitator for today, Miss Summer Fowler. Miss Summer is a technical director with the CERT's division risk and resilience management directorate. Summer, welcome, all yours.

Presenter: Thank you so much, Shane. Yes, good afternoon from sunny Pittsburgh, Pennsylvania. Thank you so much for joining us on this webinar to announce and discuss an exciting new program that we have here at Carnegie Mellon University. At Carnegie Mellon's Software Engineering Institute, we work closely with both public and private organizations. And they're constantly faced with hurdles that inhibit their ability to successfully implement a fully integrated risk management program.

## Business Risk

CERT | Software Engineering Institute | Carnegie Mellon University [Distribution Statement A] Approved for public release and unlimited distribution. 4

**004 There are a wide range of risks to businesses and organizations, such as market, regulatory, financial and now cyber risk.

## CYBER RISK

[Distribution Statement A] Approved for public release and unlimited distribution.

**005 Realized risks in recent years have revealed the need for a dedicated executive, or a chief risk officer, to oversee these risk management activities. However, organizations are finding it difficult to find professionals that have a broad and independent view of the organization, can be a strategic thinker, and also the ability to anticipate potential disruptions into influenced decision making.

Even more elusive is a professional with experience and an academic credential in this space. So, today our webinar is going to talk about getting that academic credential through this program. To support the growth and development of the chief risk officer role, the CERT division has partnered with Carnegie Mellon University's Heinz College of Policy and Information Systems--

## cro

CERT
Carnegie Mellon University
Heinz College
cro
Carnegie Mellon University
CERT | Software Engineering Institute | Carnegie Mellon University
6

**006 And its Risk and Regulatory Services Innovation Center to develop the Chief Risk Officer Certificate Program to provide domain leaders with the latest skills and practices in enterprise risk management.

The focus of the new program, which launches this fall, the fall of 2017, is on what CROs need to know to thrive in their jobs, including how to interact with executive leadership and how to analyze and dispose of enterprise risks. So, to discuss more about the role of the CRO, we have a couple of experts with us today. We've asked Brian Schwartz of Price Waterhouse Coopers to join us. Brian is a partner with PwC and leads the firm's risk management and compliance solutions for risk assurance in the U.S. He is also

PwC's national leader for GRC technology enablement. Brian drives PwC's annual risk management study, Risk in Review, which explores trends in how boards and the C-suite manage and monitor key business risks in relation to their strategy. Brian is a frequent speaker at national risk compliance and audit conferences and has authored articles on risk management concepts.

He holds the following professional certifications, certification in risk management assurance, certified risk professional, certified bank auditor, and certified financial services auditor. Brian has earned his MBA and Bachelor's degree in finance. So, we really welcome you and thank you for taking your time. So, thanks for joining us, Brian.

Presenter: Hey, thanks for having me here, Summer. I appreciate the introduction. I spend a lot of my time these days speaking to chief risk officers and board members helping them to sort of take their risk management efforts to the next level. So, I'm excited to share insights today with you.

Presenter: Great, thanks. So, we have a series of questions. But again, as Shane had noted at the beginning, we definitely want people on the webinar to interact with us. So, if you have questions throughout any of the discussions that we have, send them in the chat window. And we will respond. So, Brian why is the topic of risk management such a big focus for companies today?

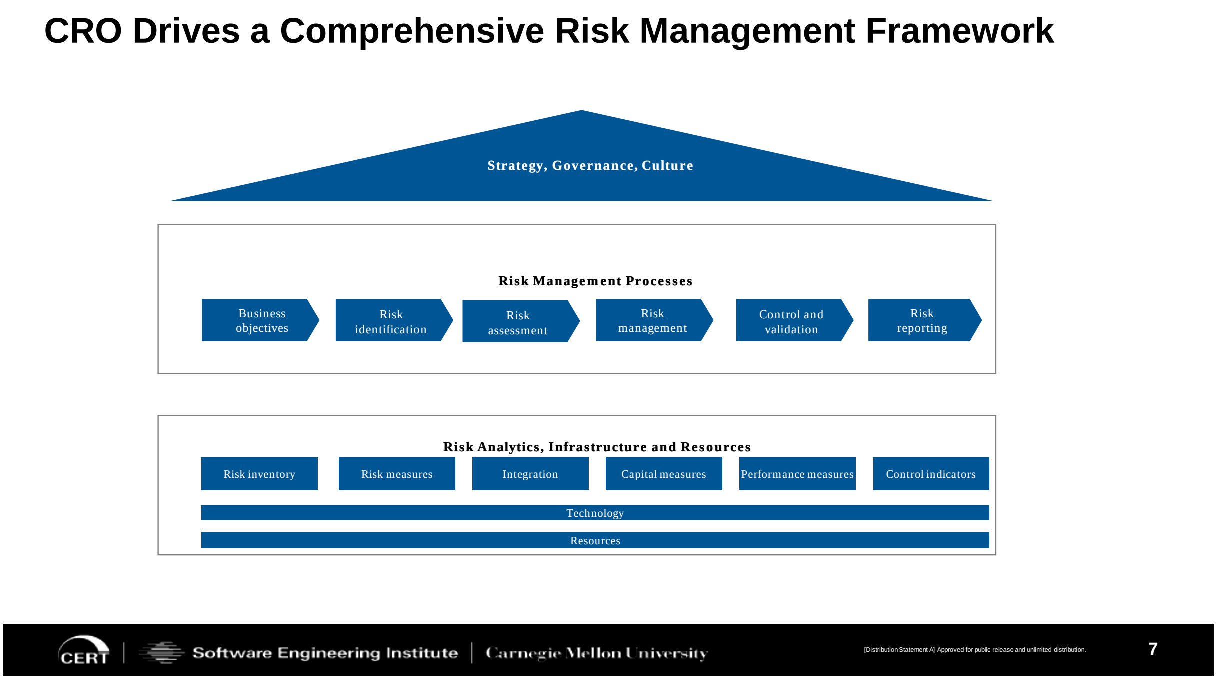
Presenter: So, where should I start with that one? PwC does an annual global CEO survey for the chief executive officers globally across industries and sectors. And what it has pointed to the last couple of years is that there's actually-- CEOs feel there's more risk out there even compared to opportunities. And that's not to say there aren't great opportunities. But it speaks volumes around the amount of risk that companies are dealing with today.

If you think about risks in certain categories, you think about cyber and broader IT risk. You think about compliance risk. You think about financial. You think about strategic and operational risk. Risk is coming at companies from all directions, both around the company and inside the four walls operationally of the company. So, companies need to take risk management extremely seriously today, build up the programs, have the right folks within the company driving risk management. And that's why it's such a big topic.

Quite frankly today, unlike five years ago, having risk management and having people in the company who focus on risk management is really table stakes. Stakeholders, like regulators, and board members, and other third parties expect certain things to be done from a risk management standpoint, that's why it's topic in the board rooms.

Presenter: Great, and because of that topic, and because of the need for this, we've seen the emergence of this role of a chief risk officer. Can you tell me a little bit more about what the role is, what the responsibilities are?

## CRO Drives a Comprehensive Risk Management Framework



CRO Drives a Comprehensive Risk Management Framework

Strategy, Governance, Culture

Risk Management Processes

Business objectives → Risk identification → Risk assessment → Risk management → Control and validation → Risk reporting

Risk Analytics, Infrastructure and Resources

Risk inventory | Risk measures | Integration | Capital measures | Performance measures | Control indicators

Technology

Resources

CERT | Software Engineering Institute | Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

7

**007 Presenter: I sure can. I'm actually going to use a slide or two as well. So, you'll see the slide on your screen as you're watching the webinar. So, we could spend hours talking about the roles of a CRO because they're executives who do a lot. But let me sort of encapsulate five points that capture a lot of the things they do today. And I wanted to show you a slide that you have on the screen to think about what a risk management program looks and feels like. This is PwC's way of thinking about it. But this is one of many ways to think about it. Let me just take you down from top to bottom very quickly and then relate a CRO's role to this type of program. You start at the top of the house. And you have really where the risk strategy is set. So, are you going to accept risk, eliminate risk, transfer risk, mitigate risk, or all the above? So, you have to understand the strategy around dealing with risk.

You have to have governance set, which are really the roles and responsibilities including a CRO, the board, and the like that actually have to deal with risk. You have your culture, specifically, risk culture being set at this point in the program, so the behaviors you expect employees to take when actually making risk decisions.

Move down from that top, the whole middle section, this is really at the heart of the risk management process. This is where you would identify your key business risks, where you would actually prioritize and assess those risks. It's where you would actually mitigate and control those risks, and certainly report out on how you're doing against those risks.

Move to the bottom of the slide. It's really the supporting tools and infrastructure around risk management. So, you have to have a risk universe and taxonomy that makes sense for your company. You have to have key risk indicators that track and monitor your progress against key business risks. You have to have tools and technologies supporting and surrounding your risk process. So, if you think about this as sort of the backdrop for what CROs have to deal with, it's a lot.

So, let me talk about the role. So, role number one is really to actually develop and push out that type of risk management framework to the company, to the companies around the first line, the business, the second line, the independent risk and compliance functions, and the third line, the internal audit efforts. So, it's across the entire organization. So, they have to develop and push it out. So, that's sort of number one.

Number two is around effectively challenging the business. Let me talk about that for a moment. This is a very critical role that a CRO has. So, when the business and the first line or the front lines making decisions to push out new products and services, to move into new geographies, to decide that they have top three key business risks under control, the CRO has to effectively challenge those decisions as sort of a gut check for the company. And that's a difficult task to do. You have to know as much as the business does to effectively challenge them in the right manner. So, that's sort of number two, the effective challenge role.

Number three is really around balancing the company between what I'll call risk resiliency and risk agility. In other words, resiliency is obviously the extent to which the company can isolate and recover from disruptions or risk events. Where risk agility is more towards how does the risk management program adjust, flex itself, or bend to changes in the business model of the company so it stays relevant. So, the CRO really helps the board and helps the C-suite balance between risk agility and risk resiliency. So, that would be role number three as a broad category.

Number four is really around setting--helping the company set the risk appetite framework. So, let me just step back from that just for a second. Every company has a risk capacity, which is really the risk they can take on before the company actually gets hurt. So, you back off from that capacity. And you actually develop your risk appetite. So, that's the amount of risk you want to take on to achieve your strategic objectives and to push through your strategic, and operating, and financial priorities. So, the CRO has a role in helping the company and helping the board facilitate determining the risk appetite framework. So, that would be number four.

The fifth one I'll mention is really around the board reporting process. So, the chief risk officer is the one person in the organization that has to take a holistic, enterprise-wide look at risk because nobody else is doing that. Everybody else is dealing with their relevant risk universe and their risk categories. The CRO takes a broad view across the organization, takes the amount of risk that's happening and occurring in the company, and pushes that up against that risk appetite. So, they aggregate the risk against the risk appetite and report that to the board, to other stakeholders, as well as do other reporting to the board. So, that's really the risk-reporting category. That's how I would sort of encapsulate five broader categories of what they do for a living.

Presenter: That's great. And in the module that you will be teaching as part of this program, you go through that determination of risk appetite.

Presenter: That's right.

Presenter: In a lot of cases, boards or executives are not giving the risk appetite. So, how do you determine that? How do you structure it? How do we work-- I know that's been a really hot topic lately.

Presenter: Your responsibility for CRO, a lot of pressure on that, the process.

Presenter: Absolutely. So, Shane I think we also have a question from the audience?

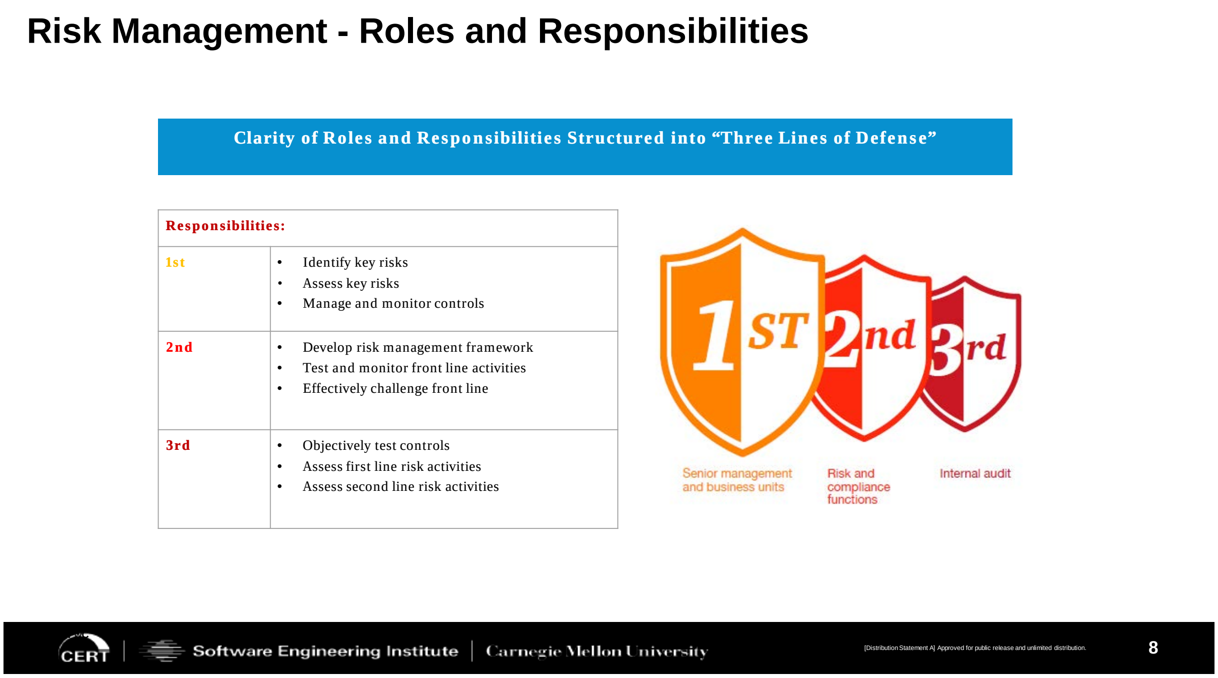
Presenter: Yeah, and it's something you kind of just covered. But we have people coming in out at different times.

Presenter: Sure.

Presenter: So, from Nancy wanting to know, "Why a separate risk officer? Doesn't that encourage large organizations to keep a department rather than showing risk as term and a track throughout the organization at every level?"

Presenter: Yeah, it's important. And listen, every company is not going to have a separate risk officer and a separate risk function. Bigger organization, that is the trend, though. The reason you want a separate executive to wear the CRO hat and not combine it with, let's say, the CFO or CEO because you do want second line independence. I talked about the second line of defense of a company. And actually, the next slide I can put on your screen as I answer this.

## Risk Management - Roles and Responsibilities



Risk Management - Roles and Responsibilities

Clarity of Roles and Responsibilities Structured into "Three Lines of Defense"

| Responsibilities: | |
|---|---|
| 1st | • Identify key risks<br>• Assess key risks<br>• Manage and monitor controls |
| 2nd | • Develop risk management framework<br>• Test and monitor front line activities<br>• Effectively challenge front line |
| 3rd | • Objectively test controls<br>• Assess first line risk activities<br>• Assess second line risk activities |

1ST
2nd
3rd
Senior management and business units
Risk and compliance functions
Internal audit

CERT | Software Engineering Institute | Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

8

**008 Every company has three

lines as I mentioned. The second line is where the CRO should sit. That's where his or her function should be. And they should be able to effectively challenge the first. If you're part of the first line, or you're part of the third line, you can't effectively challenge the first. You've basically taken away one of your lines of defense as a company. And that's not a good thing with all the regulatory pressures most companies have today. So, that's how I would answer that.

Presenter: So, a follow on question to that would be those companies that have not yet designated a CRO, what do you recommend that that they do?

Presenter: Yeah, great question, Summer. So, I spend a lot of my time in financial services. And they're the ones who have-- they're way ahead of the curve in terms of the regulatory pressure to have CROs and have formality around it. But I also deal with non-FS companies, healthcare companies, consumer products companies, industrial products companies. They also need CROs. But I always hear from them, "What if we can't designate a CRO? What do we do?" And back to the question I just answered, it's okay initially to have somebody wear two hats if you need to. The important thing is give somebody risk responsibilities beyond the business, beyond the day to day business decisions.

So, you have people-- a CFO potentially could wear the CRO hat until such time where you can actually put in a separate CRO. It makes it more challenging to effectively challenge. But it's still a good thing. And listen, every company that's successful does already manage and monitor risks. Otherwise, you wouldn't be successful. So, it's important to give that hat to someone.

Here's another way companies can do it, though. Some companies do what I call a ROC concept, R-O-C, a risk oversight committee. So, they would take-- this is at the management level, not the board level. They take a group of people, usually chaired by whoever's going to be in charge of VRM, and they form a committee. And that committee meets monthly or quarterly to talk about what the key business risks are and how they're being mitigated at the company today. And that committee can be very effective until such time as you can name a separate CRO. And when you do that, it's okay. You'll have the CRO chair that committee. But it still gets involvement from the first line, the second line, that the third line. That's how I would answer that.

Presenter: Great. So, we know it's important for organizations to have someone in this role managing the risks. But say you are a CRO or are aspiring to be a CRO, what are the important skills and competencies that you should possess?

Presenter: How much time do we have? It's a-- you all know out there, it's a tough job to have. So, here's how I would sort of talk about that efficiently here. It's really important that the person who wears the CRO hat is very deep in that industry sector where the company plays. And let me tell you why. Risk taxonomies and the relevant risks companies face, it often differs by industry sector. Okay? Some are universal like cyber. But often, some are very industry-specific. So, that CRO skill and competency needs to include depth in that industry, in that sector. That's sort of number one.

Number two, there's an inherent connection between risk management at a company and a strategic planning process because you can't strategically plan without thinking of the risks that could curtail you. And you can't do risk management without thinking of relevant risk to strategy. So, another skill would be making sure that person is deep in the company's strategic priorities. So, you can make that alignment and that connection. So, that's number two.

Number three I would say is having the credibility to what we talked about before, effectively challenging a business. You've got to have credibility in the sector. You've got to have credibility in risk management concepts to sit across the table from a colleague, someone who doesn't report to you, and challenge their decision process, not to be critical, but to be helpful for the company. You've got to have credibility as a competency.

Number four, really being consultative and collaborative. I'll even use the word collaboration because there's a trend in companies today where they're trying to integrate all the different risk assurance functions. And you've got to be collaborative with your chief compliance officer, with your chief audit executive, and with your business unit executives. You want them coming to you to pull you in. That's a two-way street. We've got to be collaborative with those people.

And then the fourth and final one I'll mention is really having superior communication skills. Listen, the CRO is going to find themselves in front of the board probably more than they want to find themselves in front of the board because that's one of the jobs, to keep the board informed. You've got to have very succinct communication skills to report what you need to in the time of a board meeting. And I'll put communications slash-- I'll put one more in it which really is influence skills because you're trying to influence the decisions that business unit executives are making when you don't have reporting relationships necessarily with that person or with those people. You've got to influence them to potentially change a decision they're sort of set on making within their mind.

Presenter: That's great. And I do know that, as part of the program, like we have a chief information security officer program, we really stress the importance of communication.

Presenter: Sure.

Presenter: And not only teach the students who are there how to communicate, but what to communicate, how to craft the message. So, the program itself really goes through those details. So, it's great. We have a question from Pam. "Where does the CRO function roll into an organization, compliance, audit, or somewhere else, especially in the case you were not able to designate independent authority?"

Presenter: Yeah, great question, and one I spent a lot of time talking at boards about because unless you have a separate and distinct CRO role and a CRO type function that sits independently in the second line, we typically see those CROs reporting directly to the chief executive officer from an administrative standpoint, but also having some functional reporting directly to the board. Whether the board has a risk committee or audit committee, it's important that they have access to the board that's really clear and concise.

When you don't have a separate CRO, and you have, let's say, a chief compliance officer and a chief audit executive type role, oftentimes a risk management person or group can report up to them. Not ideal, but again you want that smooth path to the board. But you can be under a CCO, a chief compliance officer, if you need to. You can even be under a chief audit executive, as long as he or she gives you access to the board. A lot of companies, this thing is born in the third line under the audit function. And then ultimately, it gets its own life and moves to the second line. So, there are numerous reporting lines you can take. The most important thing is get risk management up and running.

Presenter: Great. Another question from one of our guests. "You mentioned a risk event. Once a risk is realized, it's no longer a risk. Two-part question, what do you call it after it's no longer a risk? And two, does that risk event then leave the CRO's sphere of control?"

Presenter: So, every flip side of risk is going to be opportunity. So, every opportunity a company takes to push forward and to move itself forward strategically or operationally or financially, the flip side of the opportunity is going to be a risk. So, the CRO gets involved at the point of an opportunity to say, "What's the downside?" So, they can play defense but also help the business play offense by pushing something forward. Once the CRO does an evaluation and effectively challenges, let's say, the first line, and determines that the first line is making a risk adjusted or risk informed decision, they would typically back off from the day to day, but then track it enough to report it to the board. And they'll track it through key risk indicators or something of that nature that affects that decision and where it impacts, let's say, a risk in strategy and reports it periodically. But what you can't do as a CRO is take over the responsibility to manage and monitor risks. That takes you out of the second line and defeats the purpose of a CRO. You put the ownership and accountability back in the first line and just monitor through conversations and KRIs.

Presenter: Great. So, Brian you live this every day.

Presenter: I do.

Presenter: It's something you work with organizations who have CROs, organizations that don't. What would you say to people who are watching this webinar who are considering attending Carnegie Mellon University's Chief Risk Officer Program?

Presenter: First, good for you. It's not an easy role, but it's a very important strategic role. So, I commend you for even watching this webinar and to be thinking about this Carnegie Mellon program. Think about what I mentioned earlier about the intenseness around risk management for a company. Right? A corporate governance structure at a company includes risk management as one of its key components or elements. So, it's very important. CROs need to understand the latest risk management thinking around tools, techniques, approaches, methodologies, so they can do their job even better. So, whether you're in the role today, or you're watching this because you at to actually get into the role, you aspire to get into the role tomorrow, you need to take your skills and competencies to the next level. This is the type of program that will offer very pragmatic and very tangible risk management concepts where you can go back to your company and make a direct impact.

Presenter: Great. Another question before we let you go. Jake has a question. "I love the insight and have been in that position as a senior risk manager. While the position was very successful and effective, there was a very well understood us and them mentality. Management empowered me and our team to do this to the fullest extent. However, I was not given authority to make the changes with the other engaged teams, leaving us in a not complete buy-in to the concept. How does one ensure that the CRO is not only empowered, but carries authority with earned credibility?"

Presenter: Yeah, great question. I mean the authority comes from the reporting line. Like I mentioned, the CRO needs to have a direct line to the CEO and to the board in a perfect world situation. And that automatically obviously creates credibility just from a reporting line standpoint. Then if you have the skills we've talked about, you're deep in this sector and industry, you understand the strategic priorities, you understand the strategic priorities, you understand the key business risks, you're going to earn credibility by having those types of conversations and supporting conversations with the business. So, if you can become a partner of the business while keeping a second line perspective, that's a win-win for the company and a win-win for you as a CRO. So, it's very doable to do that. It's hard. It's challenging. But you can get there.

Presenter: Well, Brian thanks so much for your time. I know Brian will be sticking around until the end of the webinar. So, if you have other questions, please continue to send them. We really do look forward to your full course module in September. So, it's a thank you.

Presenter: Thanks for the time.

Presenter: Great. Now I'd like to welcome up to the webinar Greg Porter. Greg is the founder and owner of Allegheny Digital, a Western Pennsylvania based security and privacy services company specializing in network infrastructure security, digital forensics, regulatory compliance, and enterprise risk management. For the past several years, Greg has both led and delivered comprehensive assessment activities that monitor, test, and audit the effectiveness of information system security, risk managed governance and controls, and legislative conformance. In addition to his technical degrees from the University of Pittsburgh and our own Carnegie Mellon University, Greg maintains several information security related certifications and is a certified information systems security professional and a certified information security manager.

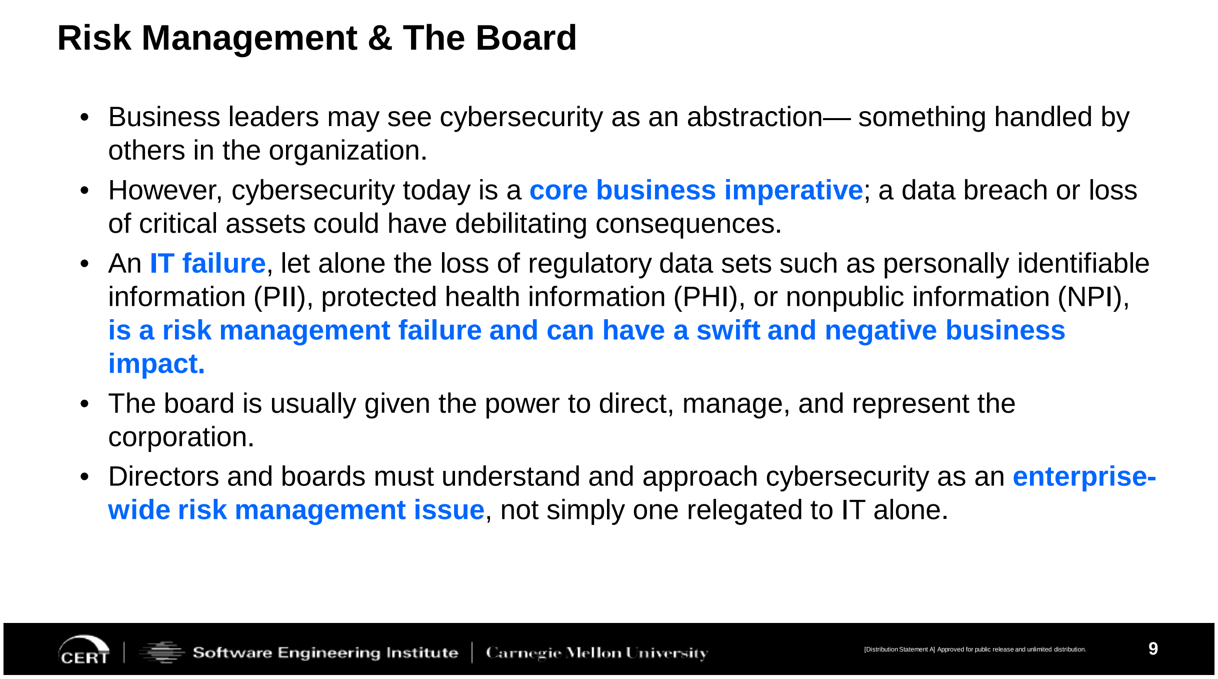
Greg, you've been a university affiliate with the CERT division of the Software Engineering Institute for over eight years now. So, you've been a great friend to us and to our programs. Greg teaches for the Chief Information Security Officer Executive Certificate program, the CISO program that we have. And he's developed a module for the CRO program, which launches this fall as well. So, welcome and thanks for joining us Greg.

Presenter: Well, thank you Summer. I appreciate the introduction and delighted to be with you here today to talk a little bit more about the CRO program, but also the important aspects that cybersecurity play in the role in terms of calibrating risk in today's business environment.

Presenter: Right. So, Brian talked a lot about communication. And a question that I have for you is how common is it to see boards informed of security related risks?

Presenter: That's a great question, Summer.

## Risk Management & The Board



### Risk Management & The Board

- Business leaders may see cybersecurity as an abstraction— something handled by others in the organization.
- However, cybersecurity today is a **core business imperative**; a data breach or loss of critical assets could have debilitating consequences.
- An **IT failure**, let alone the loss of regulatory data sets such as personally identifiable information (PII), protected health information (PHI), or nonpublic information (NPI), **is a risk management failure and can have a swift and negative business impact.**
- The board is usually given the power to direct, manage, and represent the corporation.
- Directors and boards must understand and approach cybersecurity as an **enterprise-wide risk management issue**, not simply one relegated to IT alone.

[Distribution Statement A] Approved for public release and unlimited distribution.

9

**009 I'd like, on the one hand, to echo Brian's sentiments in terms of large organizations. We see that handled often quite capably in terms of communicating at the highest-level executive leadership, stakeholders, and the board. However, a lot of the organizations that we work with really, at this point in time, are looking to achieve that degree of organizational maturity. And there's a number of ways that they can do that. But I think you kind of begin when you think about cyber in particular. If we don't have that enterprise-wide view, you can kind of start to think of cyber related risk in terms of IT only. And that's becoming more and more dangerous as we evolve into the Internet of Things, the emergence of autonomous vehicles and so forth, data everywhere on multiple devices. We really need to think about this technology ecosystem. And I think in terms of putting that a little bit in context, where does risk lie within the organization. We might not have the luxury of a chief risk officer role in our organization. And often cyber is kind of managing that responsibility.

But it really comes down to four areas I think, people, information, technology, and facilities. So, we can kind of bring that up in a broad context. But do we have an understanding of what the respective risk is in each of those areas, not just to our data and the systems, that's often most obvious, but the facilities and the people, not just our full-time employees, but maybe some external consultants that we could be perhaps working with. So, that's one aspect of it.

Now that's quite a wide base. How do we address that risk not just from a cyber perspective but enterprise wide? And that's really incumbent on having adequate staffing and funding. Now, sometimes a disconnect may arise. If we don't have sufficient communication with our board, and we're actually demonstrating things that were mentioned prior, the ability to adapt with our business environment, agility to move and not kind of remain static. That funding and that awareness starts at the board level.

We think of this notion of beginning from the top down. But if we're not communicating with our board and stakeholders, we're certainly not going to have that visibility.

So, it's easy enough to say. But again, I think from an emergent property, one of the things that we can look to do as an organization, if you're not already having maybe quarterly touch points with your board from a risk and cyber related perspective, something that you can look to aspire to. Inform the board. And almost without fail when we go into a client these days, we'll get feedback from executive leadership. A board member showed up with a recent article, or they're showing it on their mobile device. And that then becomes the important priority that they need to focus on. But there's other ways you really want to kind of advance that conversation. And I just might add quickly, one of the things that we've had success with recently over the past few years is actually inviting not just executive leadership, but board members to attend things like tabletop exercises where we can go through not just maybe a cyber related exercise but any number of operationally detrimental events. We kind of role play that. And that's extremely powerful to have the board member there that can really put the risk that might arise in context, not just digital risk but some of the other areas of the business, and understand is this an issue that we don't have adequate funding, or we need to increase staff. And that really opens up the conversation at the executive level. Had we never done those types of exercises, we wouldn't have that interaction. So, it's a good place to start.

Presenter: Great. So, Jake asked a question that I think you started to address here. "Can you please address the full extent of a CRO? Some believe it only resides in the financial aspect. But we utilized it," in his role, "To address the business units across the board of all team functions." And that's what you were discussing, that this isn't just a cyber issue. It's not just a people issue. It's a lot of assets. But can you discuss the challenges that a CRO has in addressing this and the financial aspects that the board wants to hear about?

Presenter: Yeah, sure, Summer. So, I think just in terms of Jake's question, when we think of risk, especially when I talk to cybersecurity leadership, we have to remain mindful of those four areas that I mentioned, people, information, technology, and facilities. So, calibrating risk becomes important in those areas. One of the ways that you can do that, it was mentioned, a risk oversight committee. In cyber, we do see the emergence of things like information security management systems. So, again, you're thinking of that threat horizon, that risk horizon. What are we dealing with currently, but also what's emerging? And if we don't have that vigilance or that oversight, we're going to oftentimes going to miss what's right in front of us.

And if we need a painful reminder, if we look at the events from just last week that organizations globally are often ill-prepared to meet these digital risks, and how it impacts things like life-critical systems and health care. It can be fairly significant if you take down something like an electronic health record system, or if we think of the grid as we introduce more and more technologies. So, I think assessing risk enterprise-wide, that's a good way to kind of interact with a CRO and cyber as well. Many times, you might not have that luxury of both roles. What we often see is somebody like an information security officer, for example, trying to understand what those risks are and then conveying those to executive leadership and the board.

Presenter: Right. And as part of the program, and we'll talk about the curriculum a little bit later, the CRO program does discuss how to address risk from an enterprise-wide standpoint with very practical advice, and tools, and tips, and techniques on how do you address enterprise-wide risks to be an operationally resilient organization. We know bad things are going to happen. So, what we really want to do is be able to operate through them. And that covers a whole bunch of different types of risks, as we talked about, regulatory changes, changes in the law, changes to the financial state, or cyber risk.

Presenter: It does, Summer. And I think just as a shameless plug while we have the time, for those listening, kind of what you're alluding to is how do we maintain-- what are these areas that we should be focusing on in terms of risk. Sure, it's easy enough to kind of categorize it in the four areas that I mentioned prior. However, if you're listening to the webinar, and you're looking for some resources, "Hey this sounds interesting, but you know what, maybe I'm dedicated to one certain area of the operation," perhaps it's business continuity, or it could be application development, what we've done at CERT over the past number of years is develop something called the resilience management model. I think now it's up to twenty-six process--

Presenter: Twenty-six.

Presenter: Twenty-six process areas. So, that's way that you can actually download those respective process area documents, look at how to, not only establish competency in that process area, but how do we mature that over time, up to and including board level visibility, executive presence and so on. So, you know just maybe a resource to consult if you're thinking about how do we stand up-- not just manage a CRO position, but manage technical, administrative, and physical risk within the organization because more and more we're seeing that convergence across those three areas.

Presenter: Absolutely. So, the role of the chief risk officer is an emerging one. We see more and more that companies are leaning towards having this role inside of the organization. But how do you see this role evolving or expanding in the years ahead?

Presenter: Well, I think a number of notions come to mind from my perspective.  I mentioned earlier just a few minutes ago that in middle-sized businesses that some of these organizations are still coming to terms with anointing an information security officer role. However, I think, over time, whether it's legislatively driven, there's this expectation now that you're able to capably manage risk, particularly as technology becomes more pervasive, whether it's in the cloud, IOT, which I mentioned. So, having that understanding of what those technical threats are to the environment, I see a CRO position-- It was mentioned nicely by Brian that we want to maintain visibility across all risks. But I think what I see emerging more is this notion of digital risk. How is this CRO staying informed of what those risks and threats look like?

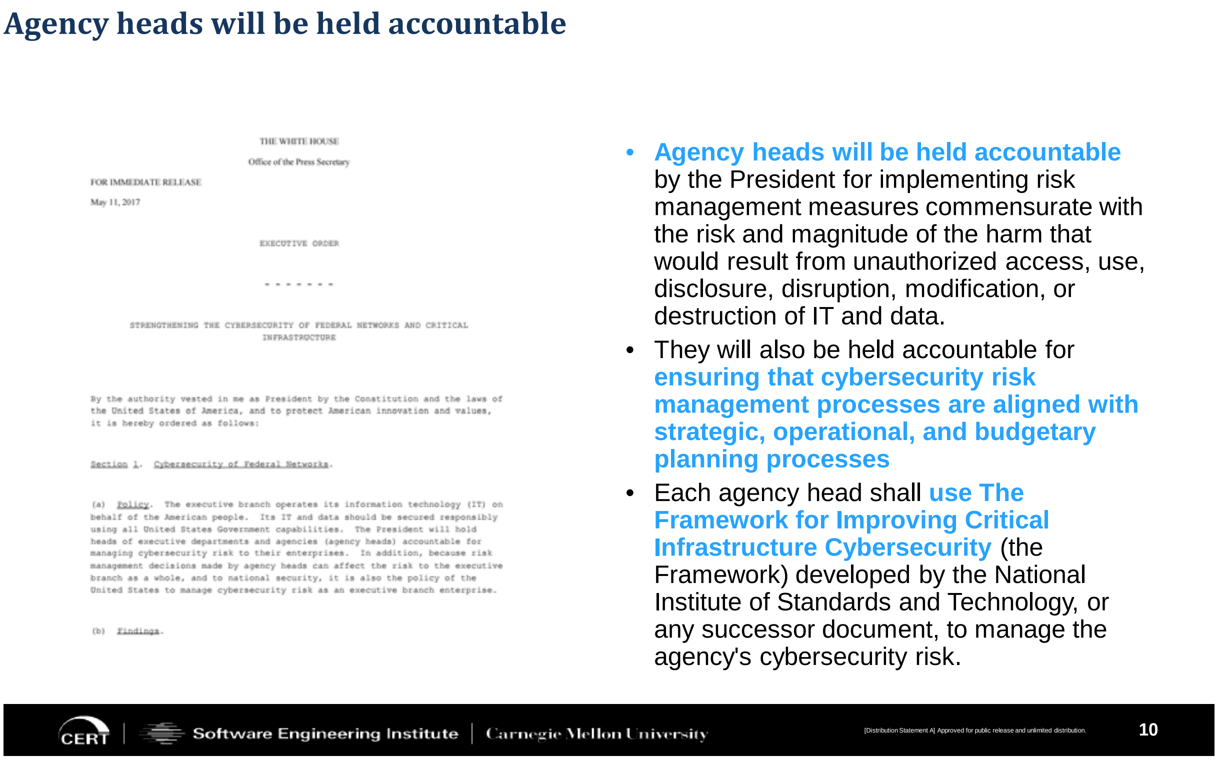
You know, naturally it's collaboratively working with somebody like an information security officer. But in absence of that, we want to have that skill set somewhere within the organization, whether we own it as a CRO ourself, or whether perhaps delegating that to other members of the team. How are we getting that input in terms of what that threat landscape looks like, and how we're managing and accounting for that risk? So, I think a cyber kind of skill set, Summer, is an aspect I see playing an increasing role into this kind of notion of a CRO position.

Presenter: So, speaking of that, you and Brian have both spoken about how important it is for a chief risk officer to be collaborative. Part of that is that a chief risk officer can't do it all by him or herself. And so, information sharing becomes a really important element of the chief risk officer role. There are organizations called ISAACs, Information Sharing and Analysis Centers, or ISAOs that are now coming out based on executive orders from the president. What value can a chief risk officer obtain from being a part of an ISAAC or participating in one of these organizations?

Presenter: It's a very good question, Summer. In fact, we often ask our clients when we go in there to do assessments, are they participating in their vertical ISAAC maybe if it's education, or health care, for example, and so forth. And many times, they're not. So, these information sharing and analysis centers are becoming more and more important in terms of the quickness and the swiftness with which technical threats are materializing in the environment. So, the way the ISAACs-- one of the roles that they can play is really using this herd mentality. What are the sensors? And I like to think of all the employees who work for an organization or work in an industry, they're really the front line risk managers. They see risks and emerging threats. An ISAAC is a wonderful mechanism to communicate maybe that initial indicator, that suspicious event. And then that can get deployed and communicated to other members of that respective ISAAC. So, it's not just an excellent resource from a cyber perspective but from a general risk management perspective. If I'm trying to maintain contact and understand what my threat theater looks like, something like an ISAAC really plays an instrumental role in doing that.

And this gives rise, the ISAAC does, to this notion of threat intelligence as well. So, the ISAAC can play a role in that. But there are certainly other private sector organizations that can provide that type of instrumentation, if you will, to kind of feed and inform your risk management processes.

Presenter: Great. So, you mentioned cyber a couple of times, which is near and dear to my heart. The NIST Cybersecurity Framework was mentioned in the most recent--the presidential executive order that dropped last week.



## Agency heads will be held accountable

THE WHITE HOUSE

Office of the Press Secretary

FOR IMMEDIATE RELEASE

May 11, 2017

EXECUTIVE ORDER

- - - - - - -

STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE

By the authority vested in me as President by the Constitution and the laws of the United States of America, and to protect American innovation and values, it is hereby ordered as follows:

Section 1. Cybersecurity of Federal Networks.

(a) Policy. The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise.

(b) Findings.

- **Agency heads will be held accountable** by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data.
- They will also be held accountable for **ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes**
- Each agency head shall **use The Framework for Improving Critical Infrastructure Cybersecurity** (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk.

CERT | Software Engineering Institute | Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

10

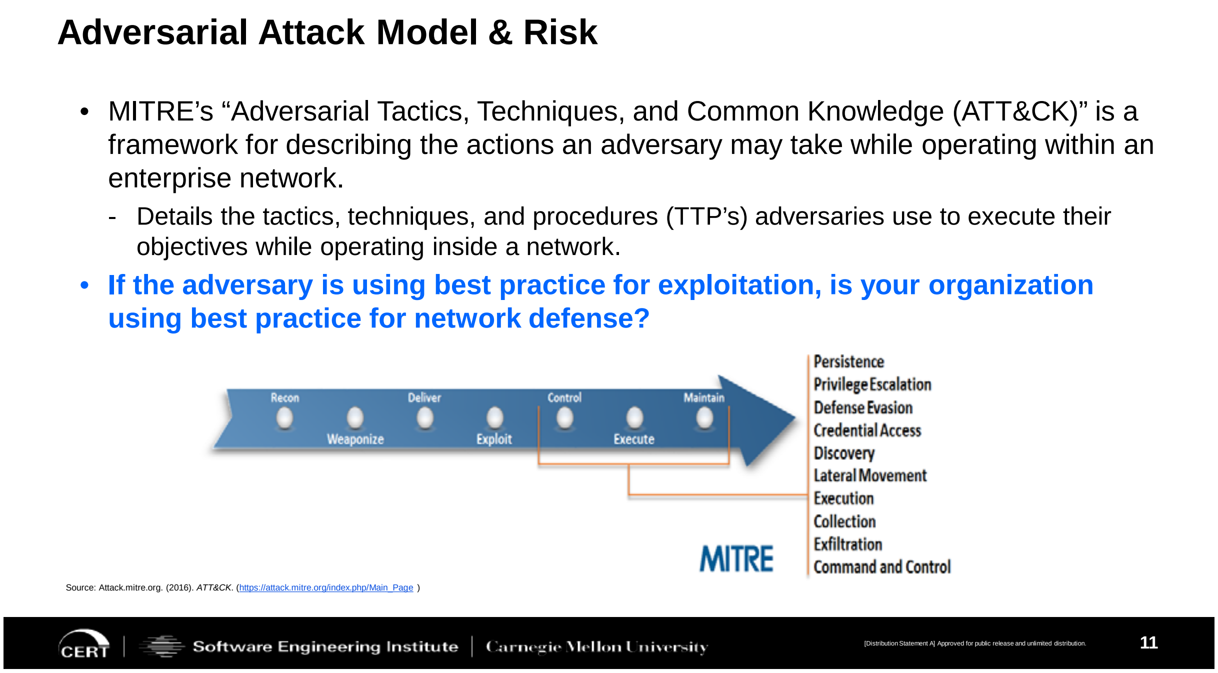
**010 So, hot off the press, we have this order from the president saying that organizations should be using the NIST Cybersecurity Framework. How does a program like Carnegie Mellon's Chief Risk Officer Executive Certificate program prepare a CRO for things like these regulations that drop?

Presenter: I think just first to acknowledge the executive order from just a few weeks ago, long overdue in my opinion, but it's great to see that. In fact, if we think about what's been going on in the industry, not just cyber, but just data protection in general, for a number of years we've had this concept of managing administrative, physical, and technical risk, whether--something that comes to mind for me is the HIPAA security rule, for example. But it exists within NERC, and GLBA, and also other applicable standards. But trying to drive accountability and ownership, from a competitive advantage standpoint, the more agile we are, the better we are at calibrating and calculating risk within our environment, if our competitor isn't doing that, we can quickly kind of turn that into hopefully an advantage for our business. I think one of the roles and the way I see the program, the CRO program, evolving is giving the students that information because you're learning collaboratively amongst your peer, but also bringing in subject matter experts who do this every day. So, it's easy to say how can we make something like risk management a competitive advantage. Those are aspects within the program itself that we cover and hopefully give students and arm them with those ideas and feedback that we've gathered through working collectively with thousands of clients and businesses across the country and the globe as well.

Presenter: Yeah. So, in addition to the NIST Cybersecurity Framework, what other related risk management frameworks do you see being utilized?

Presenter: Sure, Summer. I think just to go back on the NIST framework.

## Adversarial Attack Model & Risk



### Adversarial Attack Model & Risk

- MITRE’s “Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)” is a framework for describing the actions an adversary may take while operating within an enterprise network.
  - Details the tactics, techniques, and procedures (TTP’s) adversaries use to execute their objectives while operating inside a network.
- **If the adversary is using best practice for exploitation, is your organization using best practice for network defense?**

Source: Attack.mitre.org. (2016). *ATT&CK*. (https://attack.mitre.org/index.php/Main_Page )

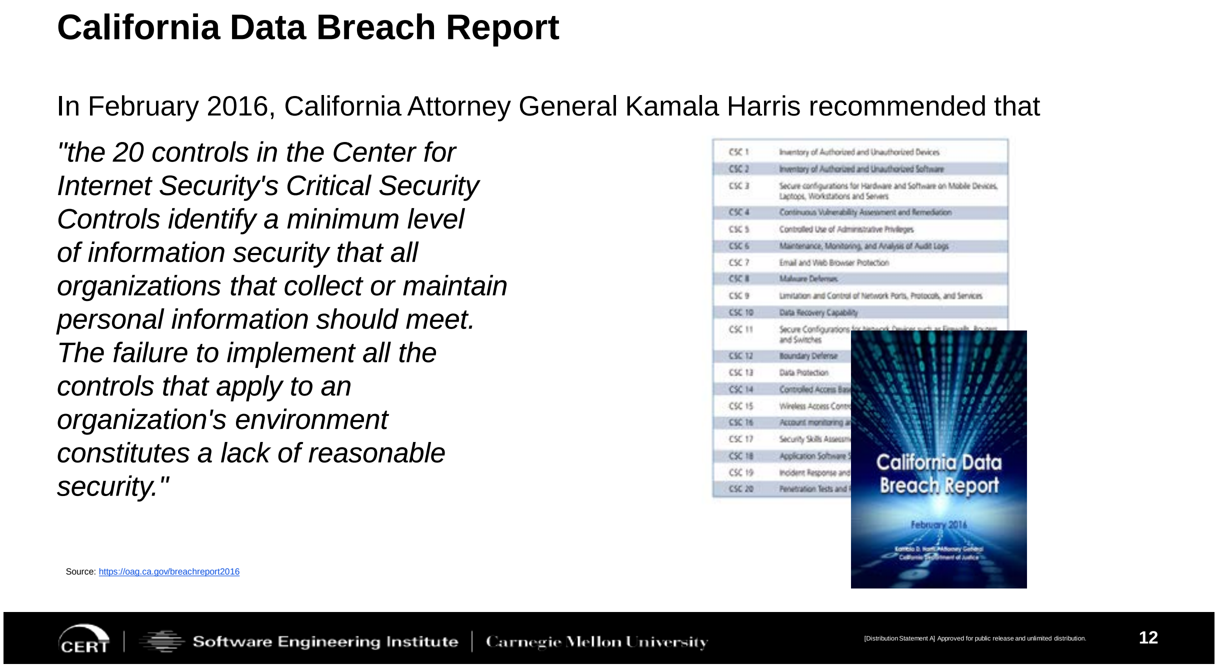
CERT | Software Engineering Institute | Carnegie Mellon University [Distribution Statement A] Approved for public release and unlimited distribution. 11

**011 If nothing else, if you're looking for a good place to start, you'll see that risk instrumentation is built into the NIST framework intentionally. It wants you to understand hey, are we doing appropriate risk analysis. Once we identify the risk, are we managing it? I mentioned earlier something like an information security management system. Some of you may be listening to the webinar here today, the International Organization for Standardization, ISO 27001. It's an excellent standard for a number of reasons. You can seek third party certification.

But beyond that, there's something called ISO 27005. So, if you're looking to build this risk management capability, you can look to this documentation, these standards, and get a consensus better practice opinion of how to build a risk tolerances, assess risk, and actually build a program itself if you're building this from the ground up. I might add just quickly there's also value in doing a simple dif or a gap analysis using these types of standards, whether it's the NIST CSF, ISO 27005, OCTAVE Allegro, which we're very familiar with here at the SEI CERT. Whatever that standard may be, or that framework, it never hurts to go back and just calibrate your own program. Do that diagnostic assessment. Are we doing these good things to meet what's considered better practice? So, those are just a few off the top of my head that come to mind.

Presenter: So, we talk a lot about cyber hygiene, and I kind of want to round out the cyber discussions that we're having. We do know that at least eighty percent of the attacks that are happening are on known vulnerabilities. So, we're not doing a very good job in the cyber hygiene realm. In your opinion, what role will the Center for Internet Security's critical security controls play moving forward for organizations?

## California Data Breach Report



### California Data Breach Report

In February 2016, California Attorney General Kamala Harris recommended that

*"the 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the controls that apply to an organization's environment constitutes a lack of reasonable security."*

| | |
|---|---|
| CSC 1 | Inventory of Authorized and Unauthorized Devices |
| CSC 2 | Inventory of Authorized and Unauthorized Software |
| CSC 3 | Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers |
| CSC 4 | Continuous Vulnerability Assessment and Remediation |
| CSC 5 | Controlled Use of Administrative Privileges |
| CSC 6 | Maintenance, Monitoring, and Analysis of Audit Logs |
| CSC 7 | Email and Web Browser Protection |
| CSC 8 | Malware Defenses |
| CSC 9 | Limitation and Control of Network Ports, Protocols, and Services |
| CSC 10 | Data Recovery Capability |
| CSC 11 | Secure Configurations for Network Devices such as Firewalls, Routers and Switches |
| CSC 12 | Boundary Defense |
| CSC 13 | Data Protection |
| CSC 14 | Controlled Access Bas |
| CSC 15 | Wireless Access Contr |
| CSC 16 | Account monitoring a |
| CSC 17 | Security Skills Assessm |
| CSC 18 | Application Software S |
| CSC 19 | Incident Response and |
| CSC 20 | Penetration Tests and |

California Data Breach Report
February 2016
Kamala D. Harris, Attorney General
California Department of Justice

Source: https://oag.ca.gov/breachreport2016

CERT | Software Engineering Institute | Carnegie Mellon University [Distribution Statement A] Approved for public release and unlimited distribution. 12

**012 Presenter: I think an important role. Sorry, it's just if we start thinking about technical security controls-- and this goes back to this knowledge and understanding that a risk officer must maintain about their environment. All these risks that we think about, okay, how are we managing technically. One of the things I like about the critical security controls is it gives us a technical prioritization in terms of managing technical risk. Now, you might look at the critical security controls and say, "Well Greg, I don't see a control for writing policies," for example. And that's really not the intent. This is a consensus opinion on how we can establish managing technical risks within our environment.

There was a slide prior to that that I think we may have shuttled over quickly. But the point is that our defensive counter measures are informed by offensive techniques. It makes sense, something so simple. But if we ask from a risk management perspective, can we go back and talk to our network security engineers, perhaps even have a conversation with our information security officer. What controls have we deployed across things like asset management, patching, incident response, data protection? And do they align with what's considered better practice? So, something like the critical security controls I think is an excellent benchmark for doing just that, Summer.

And I might just add what we're also seeing, and what we're attempting to convey here on this particular slide, is that now Senator Kamala Harris, but when she was the attorney general for the State of California, they came out annually with their data breach report. And I think it's hopefully an interesting indicator that, for those of us listening, we can ask our self within our own organization, "Are we doing these things?" And really what Miss Harris came out and stated in that report is that what is reasonable and appropriate care when it comes to cyber security, and by extrapolation, risk management. And they speak to actually using the critical security controls. And if you're not doing that, if you're not implementing these technical controls-- and by the way, if you're listening, and you're like, "Oh geez, there's twenty." That seems like a lot.

Good cyber hygiene as dictated by the Center for Internet Security is the first five. You can begin with one. But really this is what it's coming to. Do we have adequate and reasonable risk management within our organization, reasonable security?

By extension, in terms of this evolving, we can think about those of us within our respective companies that have purchased cyber liability insurance policies. These metrics, in terms of how we're extending these policies from an insurance perspective, where do we get these data points? Can we go to clients and say are you doing what's considered these good things from a risk and cyber related perspective? If you're not doing these things, that may impact perhaps negatively the premium that we're paying as an organization. And this could get to the point where it's a matter of millions of dollars. And that intern could be invested more efficiently perhaps into our risk management and technical security operations.

Presenter: Great. I see we have a couple of other questions coming in that are related to other topics. So, we will get to those for those of you who have asked questions. But Greg, I really want to thank you for taking time with us today. And if you can stick around with Brian, that will be good so that we can get some questions at the end. I want to talk through a little bit of the logistics of the program.

Brian and Greg are only two of our instructors who have deep technical expertise in the area of risk management. The program does impart applicable training, including topical discussions on current risk challenges and mitigation practices.

## cro

cro

Carnegie Mellon University

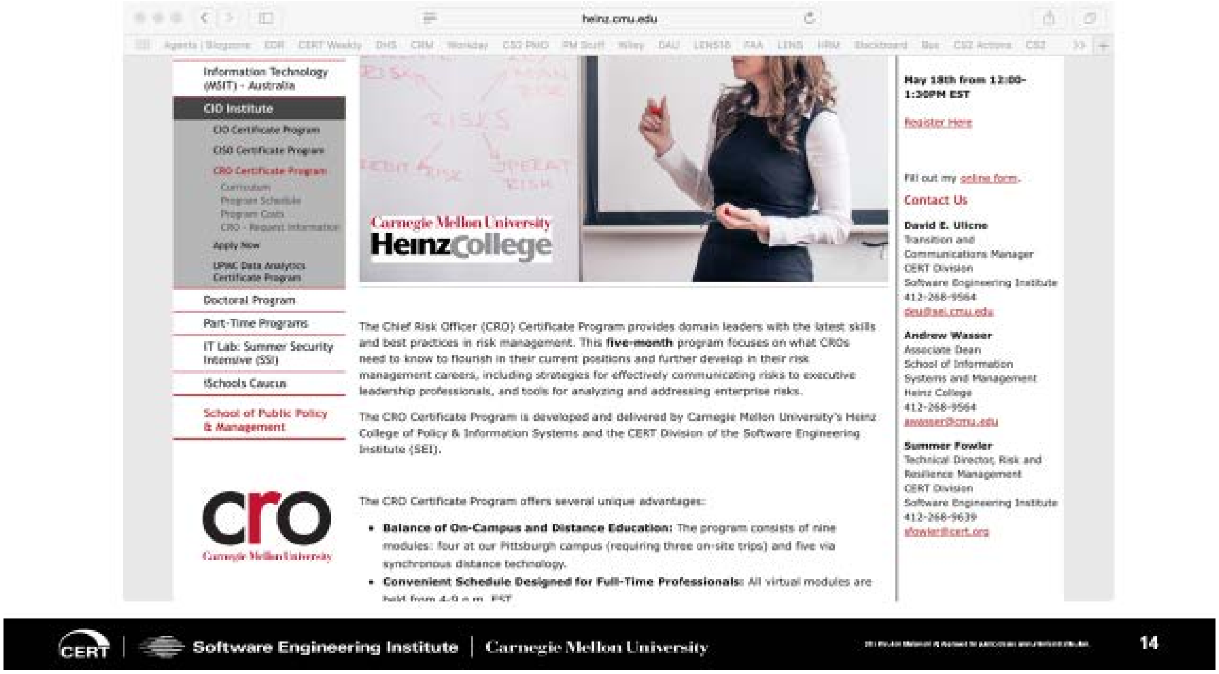
CERT | Software Engineering Institute | Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

13

**013 The learning objectives are met through a combination of expert faculty instruction, business case analyses, and active exchanges with thought leaders in the field.

## cro



The Chief Risk Officer (CRO) Certificate Program provides domain leaders with the latest skills and best practices in risk management. This **five-month** program focuses on what CROs need to know to flourish in their current positions and further develop in their risk management careers, including strategies for effectively communicating risks to executive leadership professionals, and tools for analyzing and addressing enterprise risks.

The CRO Certificate Program is developed and delivered by Carnegie Mellon University's Heinz College of Policy & Information Systems and the CERT Division of the Software Engineering Institute (SEI).

The CRO Certificate Program offers several unique advantages:

- **Balance of On-Campus and Distance Education:** The program consists of nine modules: four at our Pittsburgh campus (requiring three on-site trips) and five via synchronous distance technology.
- **Convenient Schedule Designed for Full-Time Professionals:** All virtual modules are held from 4-9 p.m. EST

**May 18th from 12:00-1:30PM EST**

Register Here

Fill out my online form.

Contact Us

**David E. Ulicne**
Transition and Communications Manager
CERT Division
Software Engineering Institute
412-268-9564
deu@sei.cmu.edu

**Andrew Wasser**
Associate Dean
School of Information Systems and Management
Heinz College
412-268-9564
awasser@cmu.edu

**Summer Fowler**
Technical Director, Risk and Resilience Management
CERT Division
Software Engineering Institute
412-268-9639
sfowler@cert.org

**014 This program is modeled after our very successful CISO executive program. We have currently over a hundred twenty graduates of our executive CISO program.

## CISO Graduate Organizations

CISO Graduate Organizations

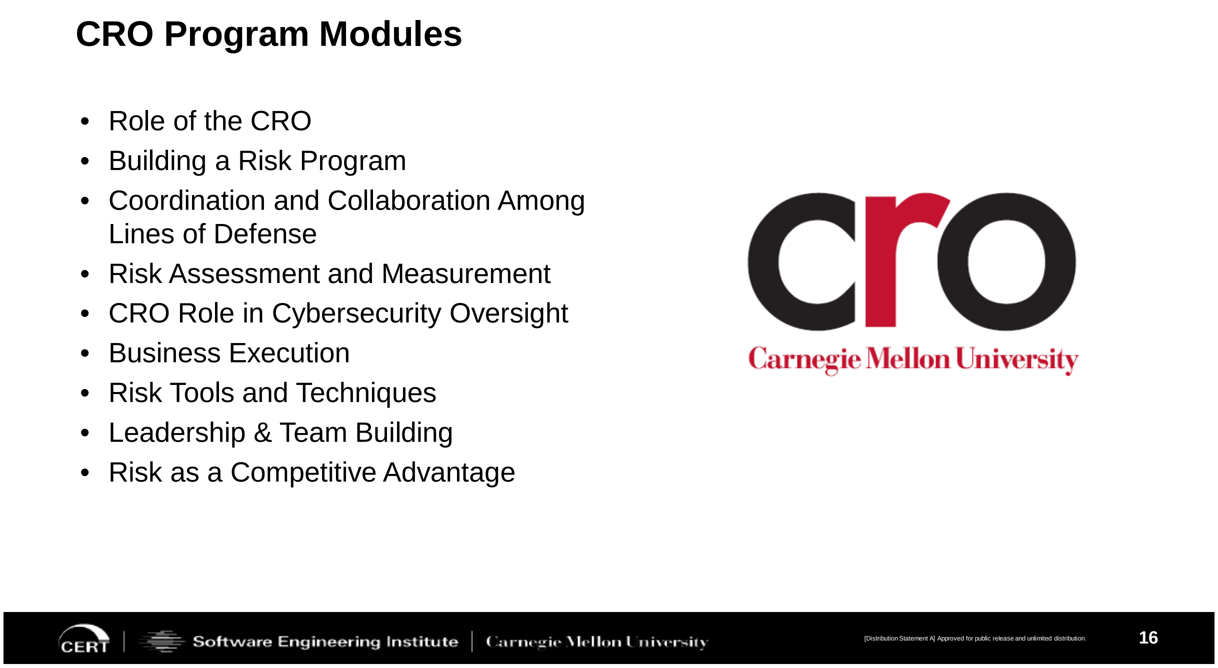
CERT | Software Engineering Institute | Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

15

**015 In the CRO program-- you can see on the side up here, we have CISO graduates from a multitude of organizations, private sector, public sector. And there are over a hundred and twenty of them. It's created a great alumni network for those graduates. The CRO certificate program is a five-month certificate program consisting of nine modules. Four of those modules will be here at our Pittsburgh campus. And five of the modules will be via synchronous distance technology, meaning you can be taking these classes from anywhere in the world as long as you have a good Internet connection. The curriculum is robust.

## CRO Program Modules



### CRO Program Modules

- Role of the CRO
- Building a Risk Program
- Coordination and Collaboration Among Lines of Defense
- Risk Assessment and Measurement
- CRO Role in Cybersecurity Oversight
- Business Execution
- Risk Tools and Techniques
- Leadership & Team Building
- Risk as a Competitive Advantage

cro
Carnegie Mellon University

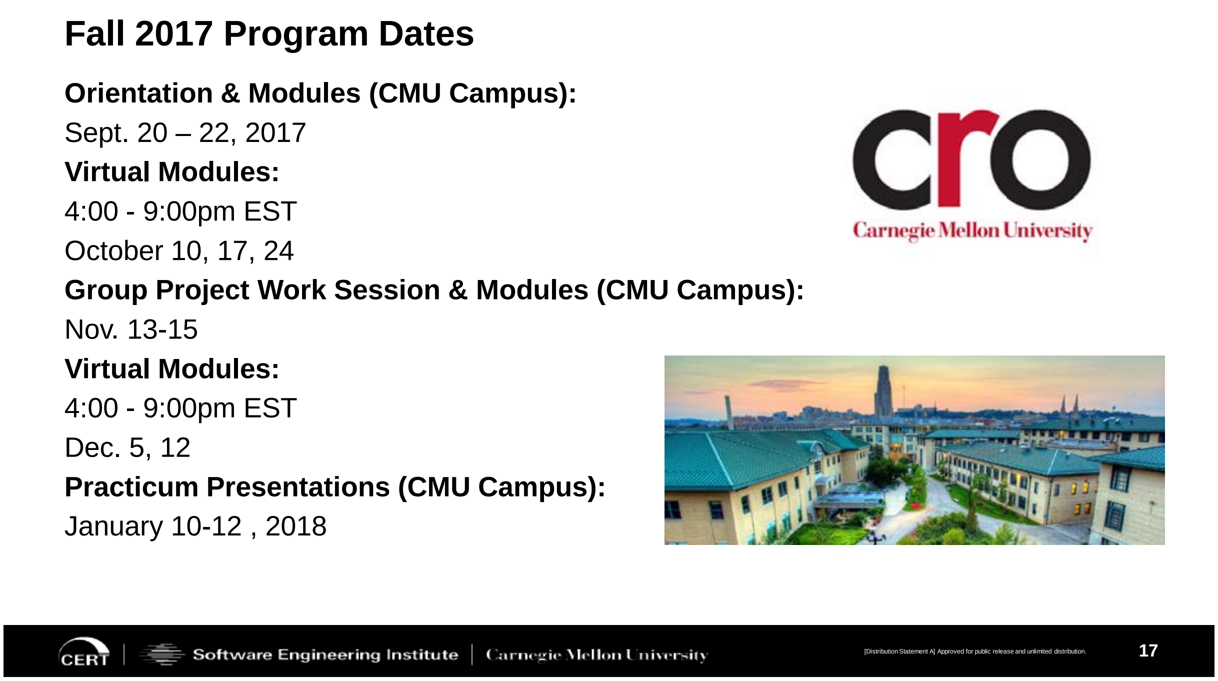
CERT | Software Engineering Institute | Carnegie Mellon University [Distribution Statement A] Approved for public release and unlimited distribution. 16

**016 It covers topics spanning the role of the CRO with Brian, who is with us today, to how to build a risk program, measurement tools, effective incident management, and even risk as a competitive advantage that Greg mentioned. So, it's a really robust curriculum that covers a lot of different topics for a chief risk officer.

As part of this certificate program, students will develop or enhance a risk plan for an organization. This is a very hands-on portion of the program. The plan is designed for students to apply several of the methods, tools, and techniques that are taught during the program, and offers that hands-on approach for executive students who we know aren't here just to have just the sole academics. But they can take something away from this that they can apply directly into their current positions.

In addition to the great faculty, the relationships that you build with other students is all a part of the Carnegie Mellon experience. You'll expand your knowledge and your network in the program.

## Fall 2017 Program Dates



### Fall 2017 Program Dates

**Orientation & Modules (CMU Campus):**
Sept. 20 – 22, 2017
**Virtual Modules:**
4:00 - 9:00pm EST
October 10, 17, 24
**Group Project Work Session & Modules (CMU Campus):**
Nov. 13-15
**Virtual Modules:**
4:00 - 9:00pm EST
Dec. 5, 12
**Practicum Presentations (CMU Campus):**
January 10-12 , 2018

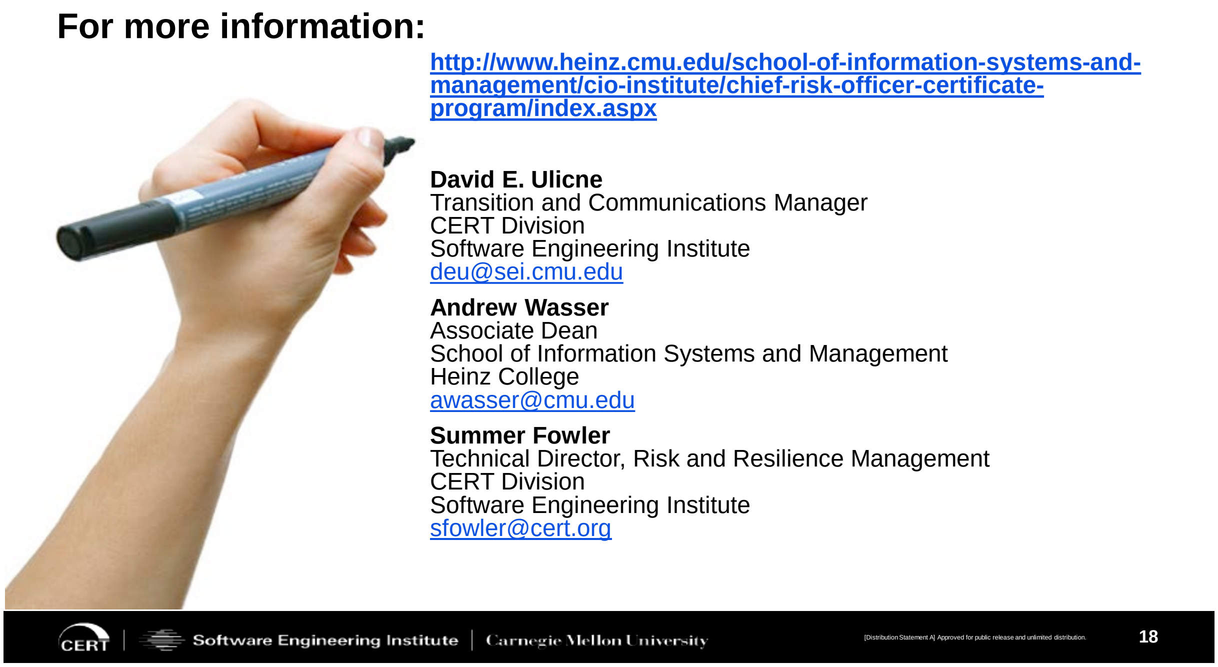
cro
Carnegie Mellon University
CERT | Software Engineering Institute | Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

17

**017 We welcome our first class of students on the CMU campus starting on September 20th for orientation and delivery of the first two modules. As you can see the schedule that is posted up before you, then there will be a series of virtual models. In the middle of the program, you come back to Pittsburgh and have another module here on site. Then there are two more virtual modules in December. And then you come back to Pittsburgh during the best time of year, January, in the nice winter of Pittsburgh. And there will be practicum presentations where you present the risk plan that you and your team put together for your assignment. We welcome our first class of students, as I said, starting this fall. We hope that you can join us for this exciting new program. And I've done enough of the talking now about the program itself.

## For more information:



For more information:

http://www.heinz.cmu.edu/school-of-information-systems-and-management/cio-institute/chief-risk-officer-certificate-program/index.aspx

**David E. Ulicne**
Transition and Communications Manager
CERT Division
Software Engineering Institute
deu@sei.cmu.edu

**Andrew Wasser**
Associate Dean
School of Information Systems and Management
Heinz College
awasser@cmu.edu

**Summer Fowler**
Technical Director, Risk and Resilience Management
CERT Division
Software Engineering Institute
sfowler@cert.org

CERT | Software Engineering Institute | Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

18

**018 I'd like to open up the line for any of the questions from attendees. I know we have a couple that are already in the queue, but feel free to submit your questions now. And I'm going to turn that back over for some of the answers to Brian and Greg.

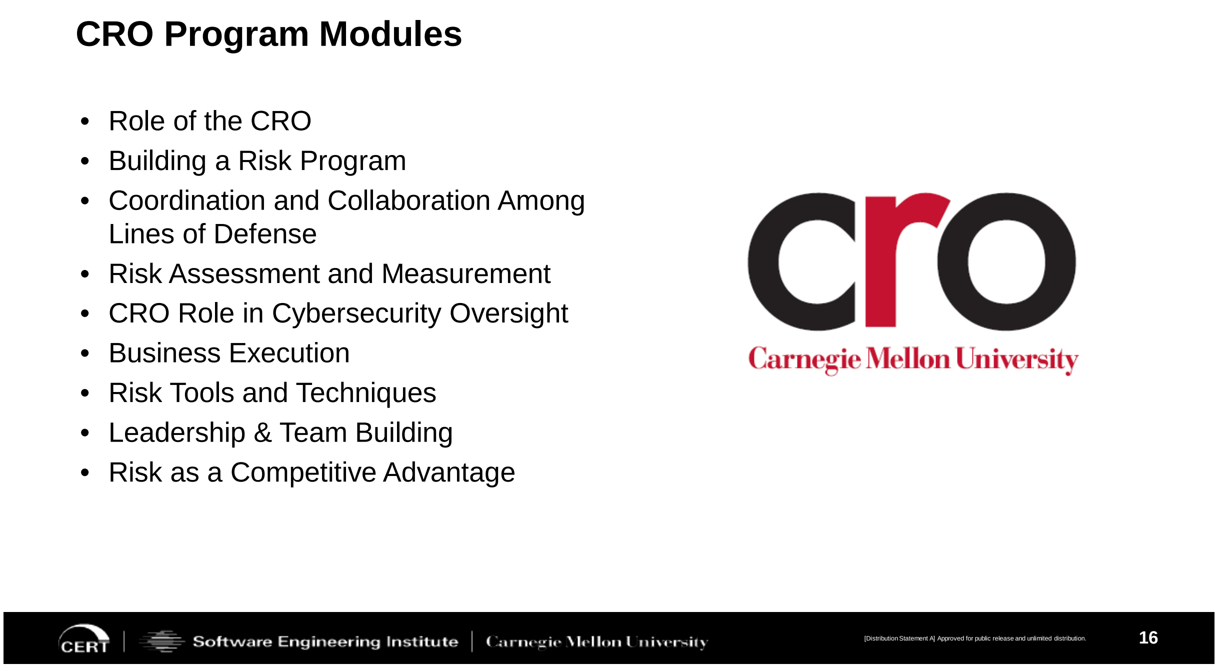
So, a question from Pam. "Does the program cover quantifying financial impact of various types of risk through proven algorithms?" So, can you discuss some of this Brian and what may be in parts of your curriculum?

Presenter: Sure, sure. We will certainly-- when we do developing of the risk management plans, the actual projects that the students will work on, we're going to actually-- part of that will be doing a full-blown risk assessment. And with any risk assessment, you're looking at likelihood impact velocity. So, the impact piece will hit financial, strategic, and operational impact. In the financial impact. We can talk about some of the techniques used by companies that get more quantifiable within an impact analysis. We'll do qualitative, as well. So, it will be in there among other things as well.

Presenter: Fantastic. And Shane, I know you have another question.

Presenter: So, yeah, a couple questions in the queue here. But before we get to that question, we also had number of questions from people asking about a replay. The replay will be available of this talk. And that will be available by this evening or, at the latest, by tomorrow morning. This will be archived. You just simply log in with the same URL and the same credentials you used to register today to be able to catch the archive.

## CRO Program Modules



### CRO Program Modules

- Role of the CRO
- Building a Risk Program
- Coordination and Collaboration Among Lines of Defense
- Risk Assessment and Measurement
- CRO Role in Cybersecurity Oversight
- Business Execution
- Risk Tools and Techniques
- Leadership & Team Building
- Risk as a Competitive Advantage

cro
Carnegie Mellon University

CERT | Software Engineering Institute | Carnegie Mellon University [Distribution Statement A] Approved for public release and unlimited distribution. 16

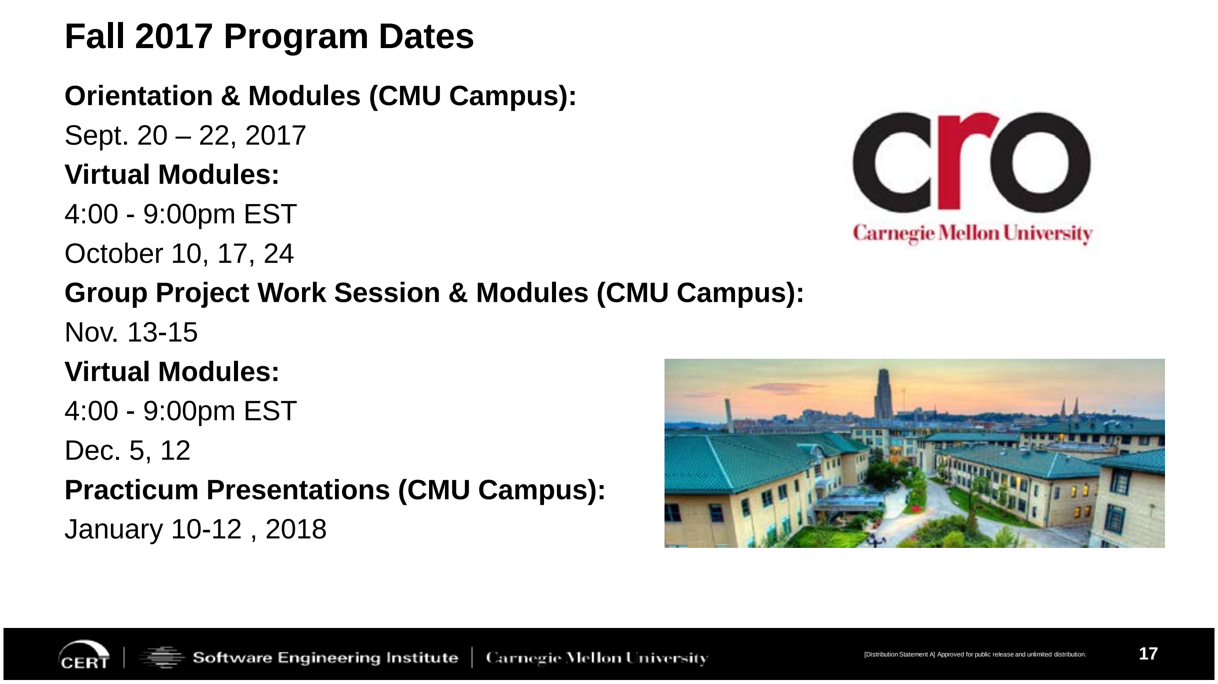
**016 And just a quick reminder, as well, please fill out the survey upon exiting today's webinar as that feedback is greatly appreciated. So, a question from Tijon asking, "How does this--" again, you talked about some of this during, but people coming in and out, "How does this role relate to the CISO role? What are the main differences?"

Presenter: Sure, I can-- you want to start?

Presenter: Yeah sure, Brian. So, in terms of differentiator, I'll speak firstly to the information security officer role. And then Brian, perhaps you can speak more to the CRO role. Historically, and this won't change for the foreseeable future, the information security officer is certainly concerned about risk. Again, if you don't have the luxury of having a CRO, you may be managing that discipline within that role internally. However, there's an important distinction, particularly when we think of large organizations, global distributed organizations, is that risk is not just pertained to administrative, physical, and technical risk that we often think about when it comes to cybersecurity. It impacts any number of areas, operational risk, financial, and so forth. And that's what I really see as the differentiator is that, if I'm an information security officer, I'm really thinking about, as I mentioned, those four areas, people, information, technology, and facilities, and how I'm managing security related risks in that context. When I start to broaden out beyond that, not that we don't consider financial risks and so forth, but if I had the luxury of having the capability of the CRO on board, I'm really going to collaboratively work with them to better understand and lend context to that type of evaluation.

Presenter: And just to add on to one thing Greg just said is that we are seeing a trend. So, in PwC's most recent Risk in Review survey and study, we saw a very clear trend that shows the CISO reporting lines are shifting. So, instead of only going to the CIO or CTO, we're actually seeing, in certain sectors, the CISO are rolling up to the CRO, or at a minimum, going alone with the CRO to the board to present the risk management state, if you will, because cyber is such an important part of that. So, we are seeing the shifting trends of CISOs and CROs becoming a lot closer, which I think is a good thing.

## Fall 2017 Program Dates



Fall 2017 Program Dates

**Orientation & Modules (CMU Campus):**
Sept. 20 – 22, 2017
**Virtual Modules:**
4:00 - 9:00pm EST
October 10, 17, 24
**Group Project Work Session & Modules (CMU Campus):**
Nov. 13-15
**Virtual Modules:**
4:00 - 9:00pm EST
Dec. 5, 12
**Practicum Presentations (CMU Campus):**
January 10-12 , 2018

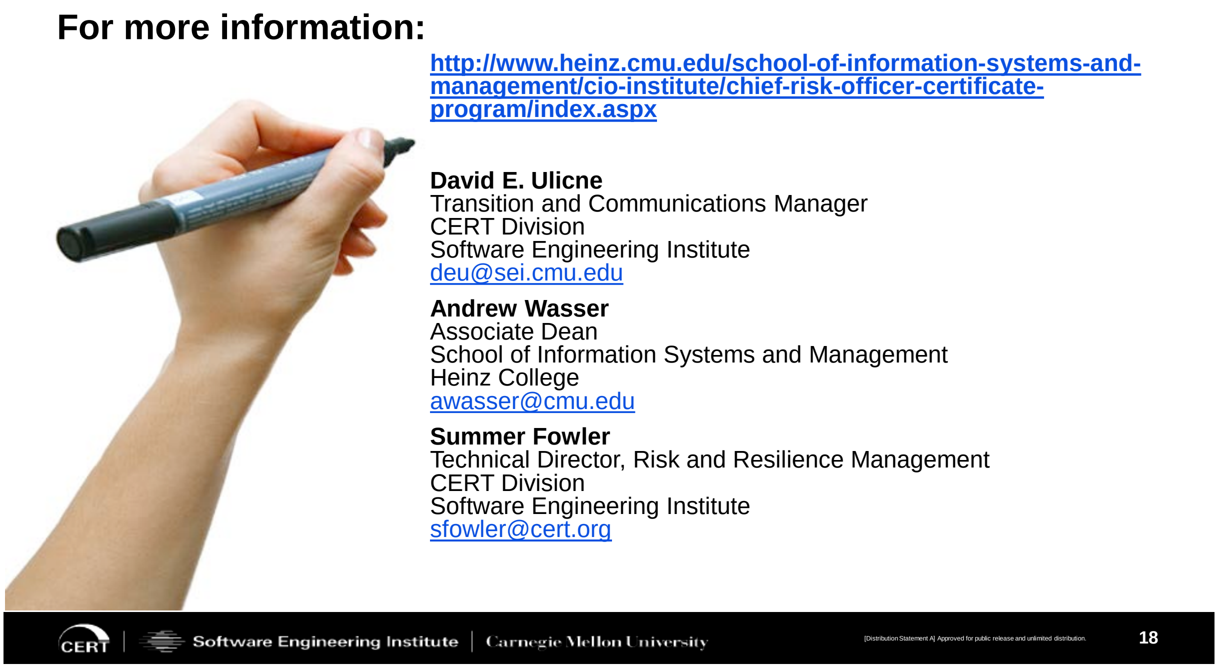
CERT | Software Engineering Institute | Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

17

**017 Presenter: I would agree, Brian.

## For more information:



For more information:

http://www.heinz.cmu.edu/school-of-information-systems-and-management/cio-institute/chief-risk-officer-certificate-program/index.aspx

**David E. Ulicne**
Transition and Communications Manager
CERT Division
Software Engineering Institute
deu@sei.cmu.edu

**Andrew Wasser**
Associate Dean
School of Information Systems and Management
Heinz College
awasser@cmu.edu

**Summer Fowler**
Technical Director, Risk and Resilience Management
CERT Division
Software Engineering Institute
sfowler@cert.org

CERT | Software Engineering Institute | Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

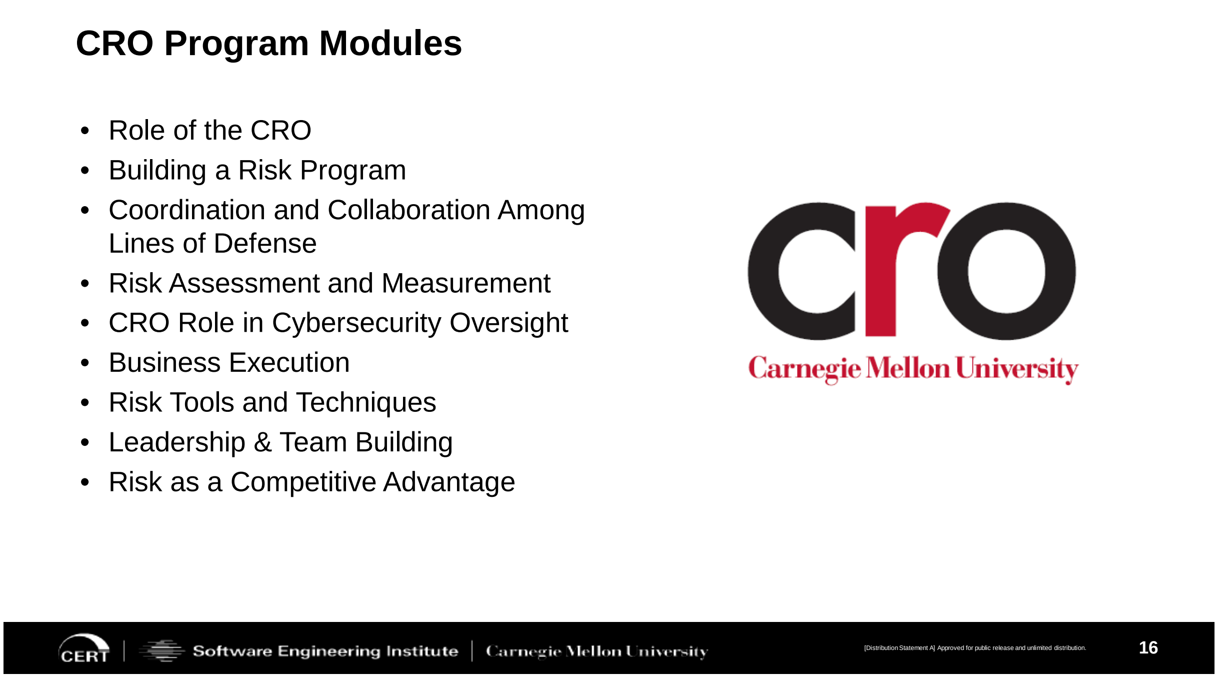
18

**018 Again, I like to think that this notion very much should be a collaborative process, ideal scenario, that you're working hand in hand with these risk officers to establish the appropriate framework for establishing risk tolerances, how we evaluate risk, and how we manage it over time.

Presenter: Another one, Summer, before I turn it back to you just asking about ROI of having a CRO role. Is there documented ROI?

Presenter: Yeah, I get asked that a lot by boards. Before we fund a CRO in a risk management function in the second line, what's the ROI? It's hard to measure the ROI of risk avoidance. So, by having a second line, and by having a CRO when he or she is fully immersed in the strategy and the risk management techniques they should use, you can dodge a lot of bullets. Right? Risk is non-stop. It's not an if; it's a when. You get hit with a disruption or a risk event, and when you have a CRO who actually has a well thought out process around isolating that risk.  Hopefully preventing it, but isolating the risk and recovering quickly from it.

## CRO Program Modules



### CRO Program Modules

- Role of the CRO
- Building a Risk Program
- Coordination and Collaboration Among Lines of Defense
- Risk Assessment and Measurement
- CRO Role in Cybersecurity Oversight
- Business Execution
- Risk Tools and Techniques
- Leadership & Team Building
- Risk as a Competitive Advantage

cro

Carnegie Mellon University

CERT | Software Engineering Institute | Carnegie Mellon University

[Distribution Statement A] Approved for public release and unlimited distribution.

16

**016 You can't-- it's almost invaluable that type of ROI. So, it's not exactly any formula. But it's really around risk avoidance.

Presenter: Yeah, great points, Brian. And I think just to add to that, and this goes back to Pam's question just a few minutes ago, and when we're thinking about trying to justify return on investment for whether we assign a risk officer role or even your information security officer position, as I like to say, "If we can't measure it, did it really happen?" And measurement really becomes key, particularly when we're conveying to the board that we're doing good things. Oftentimes, a board will ask, "Well Greg, how are we doing? I mean, we weren't hacked." And that's their most obvious thing that comes to mind for leadership in many cases. But we really want to kind of move away from that and say defensibly what can we measure to demonstrate that the investment in this role, for example, is paying dividends to the organization. And again, earlier we just touched upon it briefly, but we talked about the CRO role as a competitive advantage. The better we do at measuring, and if our competitors aren't doing that measurement, that's going to be an advantage for us because we're more agile. And we're adaptive to the risks that may be presenting themselves to our environment.

So, you might ask just quickly, and I'll add, "Well hey, that sounds great Greg. You're talking about measurement. But where do I go for guidance in terms of what I should be measuring?" I mentioned the resilience management model. Again, it's free. You can download that documentation in there. You can search for metrics-based information. There's no shortage of that. And just ask yourself a simple question, "Are we measuring these types of outcomes?" And lastly, the critical security controls, embedded within the CSEs, are also aspects of measurement as well. So, I would encourage the attendees to start thinking about how they're really demonstrating effective measurement within the context of their CRO or CISO roles.

Presenter: Great point, Greg. Just one other aspect I wanted to mention on the ROI question, I talked very briefly about risk appetite and keeping the company within its risk appetite based on where they're heading strategically. If a CRO is there to help keep within your risk appetite framework, again, invaluable because once you pass your risk appetite, and you hit your capacity, your company could be done, or it could be hard to recover from that reputation or brand damage. So, the ROI, to me, is keeping it within that risk appetite. That CRO type role helps the company do that.

Presenter: So, you mentioned risk appetite. Another question from Steve just came in saying, "How specific are risk appetite statements that are developed?"

Presenter: Yeah great, great question. And it's all over the board. I'm working with my clients on actually helping them develop a combination of a qualitative statement and a quantitative statement. So, you have to determine what's important to the company. So, one company might say, "My most important measure is how satisfied my customers are." So, that's sort of a qualitative risk appetite statement that we will not let the client-- our customer satisfaction fall below X. Or another company might have a very financial or quantitative type measurement they want to use around risk appetite that could be liquidity must stay above X. Or earnings must stay above Y. Or it could be something around regulatory standing. The risk appetite of aspects run the gamut. But my encouragement to companies is have a combination of a qualitative and a quantitative to really put around the risk appetite framework.

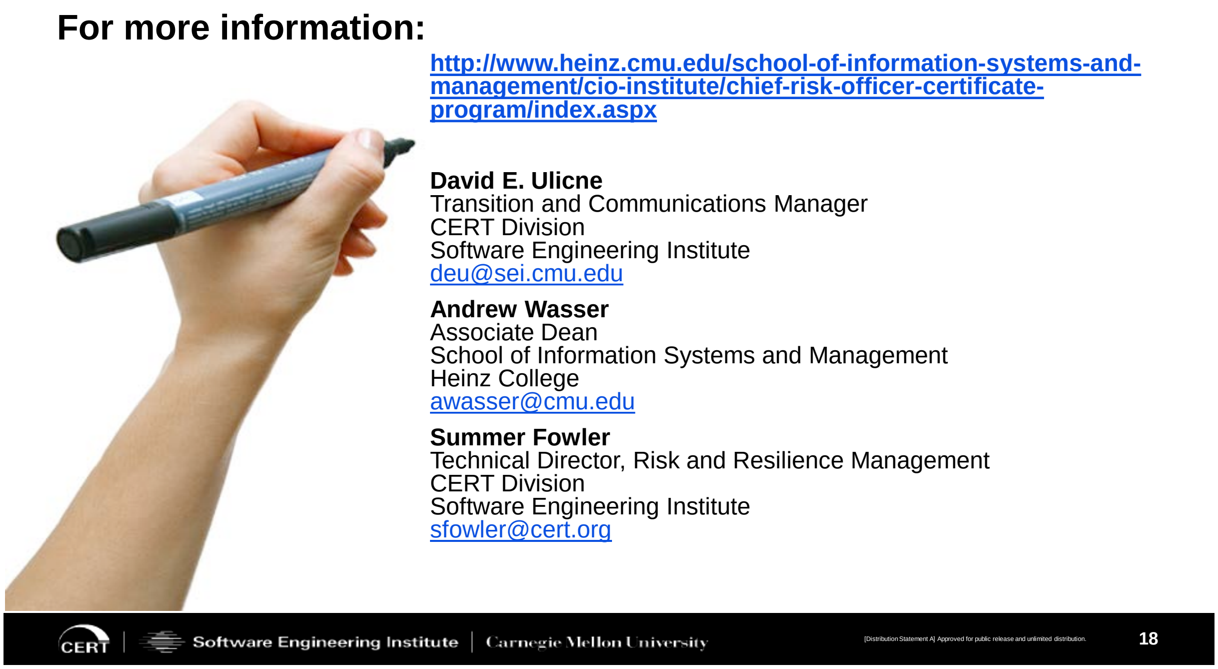
Presenter: Yeah, and Brian, something that we do in the program through both the CISO certificate programs and the CRO certificate program is teach students how to find those risk appetite statements and how to sort of cull them out of other parts of the organization. So, for example, if you're part of a publicly owned company, you can go out to the NASDAQ. And you can look at things like their 10-K filings. And you can see the risk factors for the organization so that you are speaking directly in the language of the shareholders and the board itself. If you're privately held, documents such as the strategy mission/vision statements are great places where you can start if you don't have a quantifiable set of risk appetite statements.

Presenter: Yeah, for sure, Summer. Just leave it to the cyber guy to introduce this security aspect to kind of risk calibration and so forth. But if you're going through that process, determining risk appetite, what makes sense for our business, we like to think we're all kind of unique snowflakes as an industry. But the reality is, whether you're in finance, or health care, technology, and so forth, we tend to suffer from the same types of threats to our organization. So, as we're kind of calibrating and calculating risk, I would encourage you to check out the open threat taxonomy. Again, it's open. It's free. You can look at that as you develop these risk appetite statements to say hey, we thought about this within the context of our operations. So, just a resource you consult to derive those types of statements.

Presenter: So, two more questions I have up here that are focused on some things Greg that you mentioned, while you're focus is on cybersecurity, and that's your area of expertise, you can see on the slide that we have up now the program is not cybersecurity focused, in general. It goes everything from the role of building that enterprise risk program, leadership, and team building. So, it focuses on much more than just the cyber security angle. But we do have an attendee who's asking, "How does this program address managing risks on software projects, not necessarily just cybersecurity, but on software projects themselves?"

Presenter: Well, fair question. I don't believe we have a module on software risk management. We'll touch upon aspects of that. We certainly do that in the CISO program as I shamelessly might add. But if you think about it in my module, in incident management, we talk about this interplay between things like software development, incident response, how that connects to business continuity and other resilient services, including controls management and risk management. So, I try to encourage our students not to think in a vacuum because it's their pet rock. I only work in software development. That's really what's important to me. And that's great. And we want you to be armed with the knowledge and be very capable at doing just that.

## For more information:



For more information:

http://www.heinz.cmu.edu/school-of-information-systems-and-management/cio-institute/chief-risk-officer-certificate-program/index.aspx

**David E. Ulicne**
Transition and Communications Manager
CERT Division
Software Engineering Institute
deu@sei.cmu.edu

**Andrew Wasser**
Associate Dean
School of Information Systems and Management
Heinz College
awasser@cmu.edu

**Summer Fowler**
Technical Director, Risk and Resilience Management
CERT Division
Software Engineering Institute
sfowler@cert.org

CERT | Software Engineering Institute | Carnegie Mellon University
[Distribution Statement A] Approved for public release and unlimited distribution.
18

**018 What we also want to convey through the program is this enterprise-wide mindset that we touched upon. So, how does software development impact things like incident response, continuity of operations, controls management? So, we'll touch upon those things within the CRO program to try and hopefully break that out as a differentiator to the gentleman's question.

Presenter: Great. A question from Jay Lopez, "Where can we access the CERT Resilience Management Model to evaluate?" So, that's a great question. The CERT Resilience Management Model is available for download on the SEI library. So, SEI.cmu.edu. Go to the library and do a search on C-E-R-T dash resilience management model. As an alternative, my team does develop and manage and maintain the CERT Resilience Management Model. If you look on the screen right now, you will see at the bottom my contact information. Feel free to reach out to me via email. And I can send you a copy of that document.

So, moving along to some other questions. "What is different about this program compared to other programs? Are there other programs that are available out there?" Brian, can you address this?

Presenter: I can tell you when we worked together to define this program at Carnegie Mellon, what we really focused on, and what I focused on very succinctly was a practical type solution. So, we could bring you in and talk about these risk management theories, and these quant theories, and keep it very much up here. But in my mind, the CROs that I work with, they want pragmatic immediately impactful advice and techniques so they can actually be a strategic asset to their company. So, these modules, to me, are very pragmatic. And that's why I think this program is above-- it sets the bar, basically.

Presenter: Great. Greg, anything to add?

Presenter: Yeah, I would echo those sentiments, Brian. I really think-- and I can look back on the CISO program that I've had the good fortune of being a part of from day one. The value of these programs I think unequivocally at least in my opinion is the subject matter experts that you're bringing in to teach the respective modules. These are people who are-- you're removing yourself from an academic environment and talking about practical application. What are the businesses out there today really struggling with? What are the issues? And we've already seen some great questions that the attendees have asked. Well, those are the types of situational conversations that we have during the delivery of these programs, whether it's CISO, and I'm confident with the CRO program. It's really tying theory to practice. What makes sense? What can be a differentiator for our business, by going through this program, that I'll have learned from people working in that respective field every day that I don't get exposure to maybe in my day to day role within the organization?

Presenter: Exactly. I think that's a great point. The other students, and the friendships and professional networks that are developed from the other students that are in the program is a great part. We've seen that through the CISO program. I think another differentiator for this program is how it is handled as both an on-site activity and available asynchronously via the web so that you get both the experience of being here on campus at Carnegie Mellon University three times. The world-renowned faculty, we have people from PwC, as we've noted. We have other folks from companies like Under Armour, Microsoft who are instructors. You also have faculty from Carnegie Mellon University in the Tepper school, so our business school that is really highly ranked, and then also here at CERT with the cybersecurity angle. So, that's another differentiator to the program that I see is that it really does work for busy executives. But it also does give you the opportunity to meet face to face and work with your team.

So, can you tell me a little bit more about the practicum project? That's another question we have from the audience. So, Greg, you're involved with the CISO program. And we have a practical project with that. Can you tell the audience a little bit more about that?

Presenter: Yeah, sure thing, Summer. So, again, hopefully another differentiator for the program, something unique that we do is that you collaborate with other students going through the program. As Summer had mentioned, the value in having that unique networking opportunity that you're talking to experts working across a multitude of organizations. So, what are some of the challenges that they've faced within their organization and how can it benefit me perhaps in my own practice? One of the ways we do that is through the practicum. So, we'll actually take a real world case study. Unfortunately, particularly in cyber, and certainly in risk, there's no shortage of these types of case studies to do and analyze. But most importantly, we don't just analyze it. We collaboratively as a group look at what the issue is, present that to a board, really go through with a high degree of rigor how could we have changed the outcome. In many cases, these are case studies for a reason. It was a negative event that impacted the business. What would we have done if we were in that situation? So, it creates this opportunity to learn as a group and to think about are we accounting for these types of behaviors and these potentially negative outcomes in our own operations. So, I think the practicum is just a great way to tie together all the different modules that we go through within the program and then tie that theory right to practice within the timeframe that we're actually going through the program.

Presenter: Right. I think the other great thing about the practicum project is that it allows the students to present to that board. So, it puts you in the situation where you are presenting a risk plan to that board. And it provides a nice opportunity for you to practice that. And it's a safe space also so that if you make the mistakes, you get the feedback here before you actually walk in to your board or your executive management.

Another question we have. "What is the price of the program?" So, Shane pulled this up for me here. The price of the program is sixteen thousand, five hundred dollars. However, there is a discounted rate for Carnegie Mellon University alums, CIO alums, we have a CIO program, U.S. government employees, and non-profit professionals. And that discount rate is thirteen thousand, seven hundred fifty. You can find out more information on the cost and all of the dates, again, out on the website, which is on the slide in front of you now at the top. Or you can search at heinz.cmu.edu for Chief Risk Officer Certificate program.

Presenter: I would just chime in that there's a maximum of twenty-five students per class. So, that's a--

Presenter: Fantastic. How many people are expected to be in each cohort is another-- the next question that came up. So, we do expect this fall to have about twelve to fifteen students in the cohort. Beyond that, we do cap it, no more than I think twenty-four to twenty-five students per cohort. So, it really gives you the opportunity to have a good learning experience with a low ratio of students to the faculty that you're working with. However, you then also have the opportunity to network with the other people, not only within your cohort, but across the entire alum program.

As I've noted, in the Chief Information Security Officer program we now have over a hundred twenty alums. We do hold alumni events at various conferences or here on campus. We had an event at RSA that one of our alums actually hosted at his company. And we had about sixty of the alums get together. So, that was a really nice opportunity for people who've gone through the program to meet each other. We've had really fantastic networking opportunities including people who've gotten jobs at other companies because of the people that they've met. So, it's a really great experience here at Carnegie Mellon University.

I don't-- I think that's the last question that I had as well. So, unless anyone has any more questions for Brian, or Greg, or myself, we'll wrap up the webinar. You can find more information, as I noted, out at heinz.cmu.edu, searching on the Chief Risk Officer Certificate program. In the slide deck, you will also see three contacts, Dave Ulicne, who is our transition and communications manager, Andy Wasser, who is a dean at the Heinz

College, and myself, Summer Fowler. I'm the technical sponsor of this program that is joint, again, with the Heinz program, the CERT division of the Software Engineering Institute, and the Risk and Regulatory program here that PwC helps us with.

So, I really want to thank again Brian, thank you, and Greg for your time coming in. I'm really excited about having you be a part of this Chief Risk Officer program. And I hope that many of you who have attended sign up. And we look forward to having you be a part of this program, as well. Thank you.

Presenter: Okay folks, we're going to give you a few minutes back to your day. And just a reminder our next webinar will be on June 29th. And the topic will be using Agile techniques in government settings. So, we'll send out an invite for that, as well. Again, thank you for your time today. Have a great day everyone.

## SEI WEBINAR SERIES | Keeping you informed of the latest solutions

SEI WEBINAR SERIES | Keeping you informed of the latest solutions

#SEIwebinar

Software Engineering Institute | Carnegie Mellon University