Measure and Maintain Visibility into Your InfoSec Posture
Fireside Chat Transcript
July 20, 2022

GUEST SPEAKER: Christine Horwege, Director, Emerging Technologies, CGI
4CRISK MODERATOR: Elizabeth Abraham, VP, Customer and Partner Success

SESSION INTRODUCTION

Elizabeth (Moderator): Hello everyone, if you don't know me, I'm Elizabeth Abraham, head of customer and partner success for 4CRisk, and I wanted to welcome you today to our Virtual Fireside chat where we will be talking to Christine Horwege from CGI about how measuring and monitoring improves visibility into your InfoSec Posture. This session is part of the reinforcing regulatory compliance and cognitive technology speaker series that we're having right now.

Since this is short 30-minute session, we will jump right in to asking Christine a couple of questions. We hopefully will have time to answer a couple of questions from the audience at the end of the session, so please enter your questions in the chat menu.

I want to take a moment to introduce Christine. We are very excited to have her as a part of this series. As a director within the CGI Federal Division's cybersecurity enterprise programs and emerging technology, she has over 20 years of experience successfully driving transformation through enterprise program development, implementation, and management. Throughout her career, she has partnered with government and commercial entities to enhance information, cyber risk and security programs that focus on enterprise risk, technology, data policy, and compliance. Her technology enablement focus has been on Governance, Risk and Compliance big data solutions.

Welcome Christine and thank you for taking time to share some of your thoughts with us.

Christine, you have been working with government entities and corporations for a while now. In recent years, the complexity of InfoSec has intensified. So, thank you for meeting with us today to talk about the trends you are seeing while assisting organizations' with improving their security posture and tricks they using to remain resilient in this every-changing landscape.

SPEAKER OPENING

Christine (Guest Speaker): Thank you, Elizabeth, for having me, and it's really good to work together again and catch up. I had an opportunity to watch the last month's discussion and there was some great information because Jessica spoke about their survey results, which they had collected, and there's no surprise that cyber was number one. It is a key risk and if you look at the World Economic

Forum, cyber is in the top three year over year. Information security is so critical in maintaining the business environment, ensuring that your stakeholders and shareholders alike have confidence. Now I work with government agencies today, but I've in my previous roles I've supported commercial entities as well and the risk is always the same when dealing with the confidence in the availability of services; confidentiality of information, especially personal information, with the focus on privacy and integrity of transactions and operations that lead to the two others being true.

QUESTION 1 (KEY INFOSEC POSTURE FACTORS)

Elizabeth (Moderator): Thank you. So, I want to ask you a couple questions. The first one would be what are the key factors needed to evaluate in organization's InfoSec posture?

Christine (Guest Speaker): So, I think there's a lot going on today with information security, so I really want to focus on three areas: assets, users, and third parties related to risk and compliance. In my experience, implementing information security programs, whether it's risk, compliance, or both. The key to success relies heavily on assets. This is very comprehensive today with all the hardware, software, your digital products, end users, devices, and the list goes on as you get into the network, there's just so many actors within the network that are not known or trusted today. It's really significant to think about those threats and vulnerabilities to each of those critical assets, but then your assets as a whole and also with bring your own device. What are your users doing on those devices? What kind of security settings are on those devices? The operation inside of your environment and what you're trying to control for is very focused on assets.

Today, the second is knowing those users that are operating in your environment. We have end users. You have your employees. You have contractors. You have vendors. You know with this mix you're expanding those boundaries, which is amplified by the pandemic. It is now easier than ever to work from anywhere. I currently work from multiple locations, and I'm always using multiple devices. You know this creates new challenges from an information security program. There's been a big push towards zero trust which addresses those devices' identity, workload, and data and how you're going to secure them?

I think the final is really going back to those vendors, and the cloud managed services. Your third parties you've created this whole other environment with another actor. Now, within your environment in which you have to do risk management, you have to think about compliance and how are you going to ensure that they meet your compliance requirements or your risk tolerance, and then also that shared controls and oversight that need to happen in the cloud instances.

Those are areas that we really see as bringing visibility to your program.

QUESTION 2 (DEMANDS ON INFOSEC PROGRAMS)

Elizabeth (Moderator): Thank you for that. And with the explosion of the endpoints, how does this change the demand on infosec programs?

Christine (Guest Speaker): Following along with what everyone's been saying, which is more people, better systems, and new indicators. We have so much going on that in the beginning it was more of a castle and moat, as they talk about, where you had your on-prem and your network which you could see. Here, with all of these endpoints exploding out and really being able to work from different areas, but also different devices, what you see is that information security is going to move more towards an identity base in which you have to assign an identity and then determine whether what's the behavior, what's the access, how should this be used, or how should the user be doing the work?

This goes back to all aspects, not just the end user, but also the data and the networks. What you're seeing is that it needs to be a shared workload. We're seeing a high level of effort just to keep up with how much is going on from a threat perspective; and then you know the number of vulnerabilities in the database just grows exponentially. That's why the focus of CISA and DHS is about one bringing together collaboratives in which they can collect information not only from the government sector, but also from the commercial sector. This brings a lot of indicators, like key risk indicators as well as performance indicators for those organizations, whether they're agencies or commercial; and by sharing the level of effort is really allowing everyone to utilize their workforce to the maximum.

We're really seeing that not one organization can maintain everything anymore, so the InfoSec programs are vastly expanding. It needs to include everyone. It has to be a cultural change and it has to be a tone from the top in which everyone is a first line for security in the organization, everyone is acting in the best interests of security and becomes part of that InfoSec program.

QUESTION 3 (RESILIENT POSTURE)

Elizabeth (Moderator): Thank you. So, how do you identify the right approach to maintain a resilient posture?

Christine (Guest Speaker): In my experience over multiple years of not only implementing but developing these programs, you always go back to the three major components, which are people, process, and technology. This is always going to be supported by your policy that's provides management expectations of performance architecture, regardless of your architecture, security, or operating models, which rely on the effectiveness of exchanges, policy enablement of operating securely, regardless of that model that you pick. So, it really goes back to what are your key processes? Who are your end users and what should they be doing? And then what are your technologies that you're putting into place?

What we were seeing when we worked together in the GRC initiatives, was this opportunity for an aggregate set of data. Today big data is used more and more, and we're seeing a lot with the hybrid cloud environments and exchanges, where reference points can be used to run continuous data processes. This keeps the information fresh, provides insight into how you can manage your InfoSec posture, while not only gaining visibility, but also respond appropriately.

QUESTION 4 (TOOLS AND TECHNIQUES)

Elizabeth (Moderator): That's a great point. So, what tools and techniques do you use to measure and maintain?

Christine (Guest Speaker): I would say that one of the things you're going to see with tools is that there are so many technologies out there. I'm not going to go through the list of them, for measurement, you're going to have your vulnerability scanners and you're going to look for those vulnerabilities and measurements. They've definitely done a better job at creating a risk-based approach behind those vulnerability metrics that are created today and how the solutions are handling them so that you can prioritize. The other way is I always say go back to the basics, which is to align to your business objectives and also your organizational risk tolerance or appetite depending on what you set. That really helps set those risk indicators and based on your operations and critical path processes. If you're measuring something that doesn't matter, then you're really putting your resources behind the wrong activities. It goes back to what are you aligning to. Is it in your business plans? What you fund often matters, and so thinking about your allocation of resources is really how you're going to better measure and maintain?

I can say, though, that from a maintenance perspective, we again are seeing a lot of tools that are getting better using automation to monitor compliance baselines and using machine readable languages like OSCAL, and NIST is really driving hard on this. It reduces activity that people need to do, and strain on your resources. Then compliance becomes more about security rather than checkboxes because you're doing continuous monitoring and you're out there looking for opportunities to improve those controls. It reminds me of the GRC term control test once, satisfy many that we started off with because when you meet your business security objectives, you're going to address your compliance and your risk issues, as well.

QUESTION 5 (GOVERNMENT VS CORPORATE CONCERNS)

Elizabeth (Moderator): Thanks. So, since you've been working both on the government side and on the commercial side, can you tell me do government entities have different concerns around information security than public corporations?

Christine (Guest Speaker): I would say what we're seeing is no. Government and private industry, as I was talking through CISA, DHS, and NSA collaboratives, we're seeing that the combined effort is actually showing everyone is seeing the same threats.

Having state actors behind Log4j and SolarWinds is showing that everyone was impacted whether it was the commercial side or government side.

I was reading today an article on Defense Scoop, where the Pentagon and DoD are pushing towards rapidly deploy commercial technologies. That's where you're going to see improvements in bringing automation to market and the constraints associated. How do I ensure that all my resources are used effectively and efficiently? How can I bring it all together?

It's really becoming a collaborative effort where you see government has all the same risks. They're using the same vulnerability exchanges as the commercial entities are, and also looking at the best responses. That has to be a united front from an organizational perspective, whether government or commercial entity. How do we respond to these threats so that ransomware cannot run rampant through the systems? Additionally, what I am seeing is messaging from agencies today, they're moving away from the compliance checklists and towards the risk-based decision-making and taking that risk approach, so it's really about prioritization, continuous diagnostic, and mitigations, and understanding how you're monitoring and then managing and maintaining those controls.

QUESTION 6 (COGNITIVE TECHNOLOGIES FOR INFOSEC)

Elizabeth (Moderator): Got it. So how do you see cognitive technologies like 4CRisk fitting in and supporting information security?

Christine (Guest Speaker): So, if you go back to the multiple points that I mentioned around continuous monitoring, consolidation, and convergence of data, cognitive technologies like 4CRisk are enablers of these big data consolidations. They really allow you to put together some good models. They provide opportunities to automate more activities that allow your resources to do more strategic and more evaluation and analysis versus just constantly spending more time churning on collecting the data, putting it together, trying to decipher does it go in this category or that category. And I think what you're seeing with cognitive technologies is that they provide support for that behavior I was referencing. If whether it's data or users, you're really looking for those changes in behavior or your operating environment being able to trigger the organization if they need to change or respond, or again be resilient because they have been breached.

These are things that are going to be much more effective. If I have a cognitive technology that is able to set-up models and tell me ahead of time or do scenario-based planning for me that what am I actually looking for or what should I expect to see, and I think if you look at your MITRE att&ck models where they show how to identify actors by typically behavior, it's very similar here. Where if you use a cognitive technology, you can start to identify where you have changes that aren't typical to your system, or you can start to see where a scenario may play out and you're able then to respond appropriately.

QUESTION 7 (EMERGING TRENDS / CHALLENGES)

Elizabeth (Moderator): Thanks, OK. So, what are some of the emerging trends and or challenges that you see around InfoSec or compliance programs?

Christine (Guest Speaker): I'll kind of take this from a 2-prong approach. I'm seeing a lot of technology as we'll talk about it from a technology perspective. For Infosec, the field out there is very full of technologies and managed services. What we're seeing is they're moving more towards a consolidated and converged platform, so it's not only about compliance, it's not only about security and privacy, but how do I manage all of those and multiple activities with one solution in order to maximize my resources? Because what I'm also seeing is that you really have that challenge of resources. It's not only about the workforce, but also how skilled are they? Do they know all of the

tools and technologies? How many activities can they truly do, and then how many threats are out there? What's that expansion of your workforce?

So, if you think about the digital footprint and hybrid clouds and all of the activities that are going on today, compliance becomes so complex that from an information security posture you really want to be able to maximize your resources; and so the challenge is making sure your workforce is not fatigued. I've heard this term many times, which is technology fatigue, workforce fatigue, because you're operating 24/7 for security operations centers. Threats are coming out at all hours. You have exploits that are bringing down your systems, like a colonial pipeline. I really see it like you put a fence around your yard, and you have this nice white picket fence, and it looks great. But as it starts to wear down, you start to pull pieces off it, and what you're starting to see is that your fence starts to break down over time. It's similar to your organization. You have been constantly putting up that effort, new tools are coming out, and they're constantly replacing the fence boards, replacing in the sense that activity gets tiresome. So, what we're seeing is fatigue, and from a challenge we need to look at how we can maximize those tools as they start to unify more into one platform.

QUESTION 8 (ONGOING VISIBILITY)

Elizabeth (Moderator): All right, thanks. So, you speak about the consolidated continuous approach. What is the value of having an ongoing visibility versus some point in time?

Christine (Guest Speaker): Continuous is the act of always measuring and putting into context when we talk about where those threats are or what the operating environment is and vulnerabilities. What are those responses that you need to have ready or that you need to be prepared to do so from a continuous approach where can we be looking at the operating environment, where can we look at our technology, and where can we understand where we need to respond or where we need to stop doing activities?

Risk is tricky because you don't know what you don't know, and as you think about all those risks out there that you're starting to manage, compliance is never going to cover everything. It's really just the baseline. Your information security program really needs to give you visibility from a continuous monitoring basis. How do I automate looking at my solutions, looking at my network, or looking at my user behavior? What does that look like? It's going to enable me to see those changes or potential discrepancies and be able to detect when some an anomalous activity is happening, then I can respond appropriately or recover again. Sometimes, we get hit with that exploit and we have to recover, so how do I respond to that? What am I going to need to be able to do and that brings in resiliency?

When you think about point in time, and all I ever think about is end of month, we run to the end of the month to do reporting. I used to support a CFO Group, and they would run end of the month, and everyone was downloading as much as they could, putting together the numbers and you had all those notes at the bottom. Well, that's a point in time. Now you're already into the next month and you're already trying to make the numbers for the next month, so it's, well, I have all these notes, but what am I really able to do with that? Am I able to respond appropriately? I don't see point in time

being that effective in that your response is delayed and then you're becoming reactive to a lot. Again, with so much activity and so many threats and vulnerabilities going on, you don't have time to constantly fall behind one or two steps. You have to be able to keep up with at least the minimum the high ones.

QUESTION 9 (CGI Approach)

Elizabeth (Moderator): Can you tell me how your organization CGI is approaching cognitive technology for security?

Christine (Guest Speaker): CGI, and I work with a cyber security group, we're actually looking at a lot of opportunities for data exchanges that are secure, block chain concepts and then continuous authorization and automated risk management. If you think about continuous authorization or authority to operate as we do in the in the government sector as you bring on new technologies, new systems, and new solutions onto a system onto a network, the government looks for that authorization and accreditation of the system, saying that it is secure. You're meeting the minimum controls. You have to understand your risk. What we're doing is automating that and looking to make it is a continuous approach, in which you can leverage your automated technologies around cognitive as well as the continuous diagnostic and mitigation programs that we have going with agencies today.

We are looking to dashboard all the critical risks by putting them in context, and that's where the continuous comes in. Once you understand the context in which you're operating, you have your critical assets or high value assets, you have those threats that are going directly after them, and then you understand the vulnerabilities to them, you can respond appropriately and really focus your resources versus trying to cover every asset across your network. It comes down to this idea of automating a lot of the activities of data collection and consolidation, then putting them in categories. We used to work a lot with taxonomies, understanding how those taxonomies offer or impact what you're doing, allows you to understand the visibility and those factors that are going to drive the change in your information security posture.

Then of course, you always have the converging security concept, which is if you have compliance today how can you think about security, compliance, risk, privacy all at the same time and really think about building that into my processes, so that I am not doing a stage gate approach of security steps then moving on, but I'm really building it as an underlying factor and security is really part of my core team.

QUESTION 10 – AI HELP IN COMPLIANCE (FROM PARTICIPANT)

Elizabeth (Moderator): Got it, thank you. Is the cost of information security compliance going up? How are organizations optimizing their cost of compliance while they continue to mitigate their non-compliance risks?

Christine (Guest Speaker): Costs of information security and cyber are taking over traditional compliance spend, due to the controls that are most critical align with the IT/network activities.

In FY 2020, the U.S. government allocated ***$17.4 billion*** for cybersecurity. This amount indicates over a $2 billion increase from the FY 2019 and FY 2018 President's Budget for cybersecurity — $15 billion and $14.5 billion, respectively. If you query the ITDashboard put out by GSA, Investment Details | IT Dashboard, there is a category for IT Compliance, and it is growing.

As for the commercial sector, Gartner and Forrester have projected that compliance costs and headcount have stagnated but this is in relation to traditional compliance groups and assessments; as for cyber spend and need, the number of open positions has hit over 3M, getting the limited resources in a 'sellers' market is expensive.

Organizations that I have worked for and with are managing more than ever with vendor services and contractors. Due to the ever-changing landscape of technology, threats and skills, the pace of change calls for a quick turnaround. The use of managed services, cloud providers, and shared services has become the go to.

Hyperlink above: https://www.itdashboard.gov/investment-details/028-000007002

QUESTION 11 – ADOPTION OF COGNITIVE TOOLS (FROM PARTICIPANT)

Elizabeth (Moderator): Can you provide some insights into adoption of cognitive tools in the government and commercial businesses?

Christine (Guest Speaker): The adoption of cognitive tools in the government and commercial businesses is slower due to the investment in the skills and infrastructure. With the onset of cloud, we have seen the costs associated with data reduce to where it is more viable for large quantities of data collection and retention. As well, the explosion of APIs to support data aggregation and consolidation, provides cognitive technologies with the data sources it needs to make the models effective. Cost of computing power is low to where quantum computing hubs are available for research use. The adoption in the government is happening and there are several technologies that are operating, within small scopes; whereas, the commercial side is adopting much more quickly which is exemplified in chat bots, Alexa NLP (natural language processing) capability, to name a few.

QUESTION 12 – ROLE OF BLOCKCHAIN (FROM PARTICIPANT)

Elizabeth (Moderator): What is your take on the role of blockchain in information security?

Christine (Guest Speaker): Blockchain will play a significant role in information security as we go forward, supporting the Integrity of transactions. The need to be able to track dependencies in the supply chain, like software bill of materials (SBOMs), and hardware (HW) components that are manufactured abroad and moved around. Data movement across the critical infrastructure and ensuring that the industrial and operational controls are not being spoofed (Stuxnet) are continuing to be a constant requirement for security. As data becomes more critical and valuable, integrity tools, techniques and processes become very important.

QUESTION 13 – MATURITY OF CONTINOUS CONTROL TESTING (FROM PARTICIPANT)

Elizabeth (Moderator): Where do you see the industry in the continuous control testing in terms maturity?

Christine (Guest Speaker): I see the industry in the continuous control testing as early in the maturity. Thinking along the lines of a 1-5 scale (used by multiple standard frameworks) it is at a 2 out of 5. What we are experiencing is that there are some early adopters and technologies, but that they are just gaining traction. Having experienced the beginnings of GRC solutions, this is the next evolution. It took many years to mature GRC because of the multitude of relationships and data inputs. I remember the days of document management for evidence artifacts slowing the systems down; today that is not the case and the more computing power, lower cost of data retention, and capabilities around AI, this will be a growing trend that will continue to support real time assessments, automated maintenance of technical controls, and indicators for behavior changes related to risk. Many of the right concepts are in place, it will take more adoption by larger organizations to bring down the cost of development of the technology and 'case studies.'

WEBINAR SESSION CLOSING STATEMENTS

Elizabeth (Moderator): Great thank you again, Christine. And thanks to all the participants today.

From this discussion today, it is clear that having the right tools and using the right techniques will allow you to focus on key parameters that align with your company's risk tolerance and thresholds and ultimately ensure your InfoSec program reflects the InfoSec posture best suited for your company.

Again, thank you, Christine, for sharing your time with all of us. To all the participants, we hope this session was beneficial. A tremendous thanks to all of you for joining us today.

We will send a link to the recording of the session as well as a summary transcript in the upcoming days.

We also want to put a plug in for our next event on September 1st where we thrilled to be discussing GRC Chaos to Order by Using Cognitive Technology with a guest speaker many of you may know, Michael Rasmussen of GRC 20/20.

We look forward to hearing from you in the future and assisting you with understanding how cognitive technology can strengthen your compliance program. Have a wonderful day or evening!

Christine (Guest Speaker): Thank you, thank you. Goodbye.