ceocfointerviews.com
© All rights reserved
Issue: December 21, 2020

Cyber Risk Visibility on Demand

Robert Hill
Founder & CEO

Lou Carli
Chief Revenue Officer

Cyturus Technologies, Inc.
www.cyturus.com

Contact:
844-4-CYTURUS
Info@cyturus.com

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

CEOCFO: ***Mr. Hill, what is Cyturus Technologies?***
Mr. Hill: Cyturus provides an evolutionary quantifiable cyber risk quantification service where we help organizations look at their business risk associated with their capacity for cyber security and quantify where the organization should focus resources in an effort to reduce their business risk.

CEOCFO: ***What do you look at so you have the right input to come up with a solution that makes the most sense?***
Mr. Hill: Unlike many organizations providing cybersecurity assessments focused specifically on IT from a controlled perspective, Cyturus looks at the entire business enterprise. We leverage an adaptive risk model comprised of fifteen domains providing visibility across all business units. This includes a Workforce Management domain where we interview members of the HR leadership team and discuss practices related to managing a cyber-aware workforce and developing a culture of cybersecurity. As an example, we ask practices like "Does the organization have cybersecurity responsibilities identified for each role in the organization." We continue the assessment covering over five hundred practices across all fifteen domains in areas from the before mentioned Workforce Management through Risk Management Identity and Access Management all the way through assessing the overall Cybersecurity Program maturity within the organization.

CEOCFO: ***What might you look at that people would be surprised could make a difference?***
Mr. Hill: Many organizations felt they had their cybersecurity posture well established and under control. However, in today's climate when senior leader, such as the CEO or board member asks the cyber security program leadership, "Are we secure" they follow that initial question up with "can you quantify that"? One of the things that really surprises a lot of organizations is their inability to quantify their cybersecurity maturity as an organization, not just in IT.

We find many organizations have systemic gaps when analyzing the organization as a whole, not just one or two business units. Inconsistencies in policies, standards, and guidelines that have not been reviewed and/or updated. We find other organizations that have inconsistencies and immaturities in how they manage their identity and access for users, whether it be on-prem or in the cloud. We find separate policies and separate user experiences based on not only where that resource is accessing their work environment, like we found with the COVID from home situations, but also how those resources are accessing the information, again on-prem or in the cloud.

Every organization has a different set of gaps and remediation items which are outlined on a roadmap specifically designed for that organization. Lou, I am going to pass this to you because you see these from a different perspective.

Mr. Carli: I think th biggest surprise that people have is that this tool, this platform, provides critical visibility and by that, I mean, as opposed to the traditional audit and reporting which is a snap shot in time and does not reflect the adaptive nature of cyber security. Our solution is a cloud-based platform that allows executives to see the cyber maturation of their organization in real time. That is extremely important because as we know as executives and leaders in the field, our businesses are dynamic and they are continually changing. Executives consistently let us know that our way of communicating is very effective.

"Senior leadership has visibility into that maturation on an ongoing real-time measurable basis instead of waiting for an annual assessment report." Robert Hill

CEOCFO: ***What are you showing a prospective customer? What information might they want to see? How many parameters do they need to put in when they are looking at the screen?***
Mr. Hill: We have found C-levels are not interested in parameters or specific controls; they are not interested in knowing how many characters are required in a password. They want overall metrics. Are we able to measure that our resources are meeting the criteria that we have established, and are we securely monitoring those areas that could be business impactful? Instead of looking at individual specific controls or stats on a specific measurement, we focus on providing a view at enterprise level through Key Risk Indicators (KRIs) Cyturus provides a real-time Cybersecurity Maturity Index, (CMI) a quantifiable algorithmically generated cybersecurity score. By providing a CMI, 2.47 out of 5.0 as an example, we can provide the information necessary for the leadership to make data driven business decisions on where to focus resources because the data clearly identifies the areas within the business where there are deficiencies. This empowers the organization to follow a precise remediation roadmap to reduce Business Risk and as a result increase their CMI score.

When you ask what they look at on-screen, they look at a real-time high-level view of their entire organization. This allows them to visualize, "This is where we are at compared to our baseline. We have done this amount of work, these are the areas we have reduced risk over the past three months, so now from baseline to quarter end, this is the progress, this is the reduction of business risk". Then they can review this is how much we spent to reduce that risk and to improve our maturity score within that timeframe. You take the process of maturation against the cost and now you have a true Return On Investment (ROI). Many CFOs have a difficult time quantifying the actual Return On Investment for cybersecurity spend, so being able to measure it, and to show that improvement and that trend over time, really gives them an visible ROI for cybersecurity spend that is quantifiable and directly related to reduction in business risk.

CEOCFO: ***Do you find that more and more companies are looking for that information, or do they even know that it exists?***
Mr. Carli: We know, compared to the competitive landscape, that we have a unique platform that provides visibility and a subscription service that helps our clients manage the mitigation and remediation efforts. By that I mean traditionally you receive an audit report with findings, then you are expected to go do something about it, and 95% of the companies do not actually act on the remediation. They either do not know how, they do not have the capabilities, the time, or whatever it may be, so we bring that to bear with our team. We provide a platform that provides visibility with the added benefit to help manage mitigation efforts going forward.

Mr. Hill: To continue with what Lou is saying, this is a very significant differentiator because, as Lou said, many organizations perform an assessment on an annual basis. We find that there are very similar findings, or repetitive findings, year over year because organizations either do not have the skill sets for remediation or they lack bandwidth to focus on those findings contained within those annual reports. Consequently, over that twelve months a few of them get remediated, maybe those most critical, many do not. This is why you have repetitive findings year over year.

What Cyturus is able to bring to the table is a subscription where we assign a mitigation manager to that client engagement. They are responsible for those weekly status reports, monthly updates, quarterly reviews with senior leadership to ensure the client organization is making maturation improvements, that they are remediating those findings, and senior leadership has visibility into that maturation on an ongoing real-time measurable basis instead of waiting for an annual assessment report that they have historically performed in the past.

CEOCFO: ***What were the big challenges in the Cyturus Adaptive Risk Model (ARM)?***
Mr. Hill: In my former life as a consultant in this space, it was my responsibility to come in after these large assessments, dig through these 500 pages of analysis and then try to develop actionable plans, actionable roadmaps, actionable tasks and then help that organization with their limited resources implement those changes. Having spent years in this field, I realized there had to be a better way and that is exactly what we did with Cyturus. We developed a system that allows an organization to move from assessment, to finding, to roadmap, to management of the remediation, to the reporting of the progress all in a real-time SaaS solution.

The challenges were developing something that simply did not exist. We knew how to do it manually, because we had performed those functions with organizations for decades because that was how the industry worked. However, we were able to create a platform that automates much of the manual effort, and provides visibility at every stage. In addition, doing that through a SaaS platform created a portal that our customers find very useful and they are extremely engaged throughout the lifecycle because it provides them visibility on real issues within their organization which are all tied to reducing business risk.

CEOCFO: ***Are you providing one solution or are there different modules that a customer might choose?***
Mr. Carli: The solution is all encompassing, the Adaptive Risk Model, allows us to be very flexible in our capability and to address various compliance needs. When it comes to modules, we do not necessarily break it down in modules only because it is much more effective if we have wholistic approach, as opposed to a piece meal. We do not feel like we provide the necessary visibility and we leave the organization with blind spots. However, we are flexible when it comes to pricing and subscription models based on size of organization and number of employees.

Mr. Hill: Various organizations have differing requirements. Some organizations have a CMMC for the DoD, other organizations have HIPAA or PCI. We have the flexibility based on the organization, the size of that organization, the compliance requirements of that organization, the vertical or even the industry of the organization, because we deal with power companies, manufacturers, healthcare companies, to tailor the assessment specifically to their needs as an organization. However, as Lou pointed out, the service offering is the same. It consists of the establishment of a baseline, the measurement of the findings against potential business risk, the prioritization of those remediation findings, and then that remediation roadmap creation, which ultimately ties into CMaaS (Cybersecurity Maturation as a Service) solution offering that we have been talking about which facilitates improvement over time that is measurable.

CEOCFO: ***How are you reaching out and how would someone know what to look for to find Cyturus?***
Mr. Carli: There are a several ways we go to market along with several ways to contact us. Our website is www.cyturus.com, you can email us; info@cyturus.com, or you can reach us by calling 844-4-CYTURUS. But we also have a network of channel partners that resell our services. Our channel ecosystem consists of consulting firms, security integrators, law firms etc., that want to provide their clients this type of valuable service. We just recently finished a rebranding effort and new website and in conjunction with Cyber Theory that owns multiple security properties online that provide access to co-market and co-brand our services. In addition, we partner with cybersecurity technology firms such as Fortinet Technologies as a Fabric partner, to provide visibility for their clients as well. We have multiple marketing channels in the marketplace and we have found this combination to be successful.

CEOCFO: ***What has been the impact of COVID?***
Mr. Hill: One of the things that has been impacted is the way which we interact with our customers. Historically we have gone onsite and we have had in-person sessions as we go through these fifteen domains. Many companies now do not have employees physically in their office so we do not have a place to go and have those interviews. Consequently, we

have really ramped-up our video teleconferencing and our ability to do our sessions online. In the past we always said we needed at least eight or ten feet of white board space in these sessions because we do a lot of training with resources in those sessions. As we work through these 500+ Practices, many times the client resources ask why they should perform a specific Practice or why is it important? This provides gives an opportunity to educate those resources but it generally requires a whiteboard. Therefore, we have had to adjust the way in which we approach our customers and the way we do our assessments, so that has been one impact.

Another impact of working from home has, in some cases, provided resources some bandwidth and organizations have been able to take on a project like this. They have recognized their need based on the rush to provide work-from-home solutions and the potential impact to their business. They have recognized the need to look at what else could be a potential risk within their business. Their desire to understand more about their business risks has led to an increase in our business.

Mr. Carli: COVID exposed several risks and challenges to organizations. One of the biggest risks from a cybersecurity perspective was remote work-at-home efforts. A lot of companies scrambled to get their technologies, processes, and people in place, and implemented a strategy that was half-baked. After the dust settled, companies began to ask themselves “Did we do this right? That is where we started seeing a lot of traction because executives wanted us to come in from an independent third-party perspective to evaluate what they had done to roll out remote work-at-home and answer the question, what is the impact and the risk to the business?

CEOCFO: ***Why pay attention to Cyturus Technologies?***

Mr. Hill: I think the biggest thing is the desire for quantification of business risk. So many organizations have spent millions on cybersecurity, yet we have seen a year-over-year increase in mean time to identify a breach and mean time to contain a breach. You look at the statistics and we see a tremendous increase in breaches year-over-year and an exponential increase in ransomware month-over-month. What is being done and the money that is being spent by organizations, is not working. It is not effective; it may be minimizing the impact, but it is not identifying the root problems.

Cyturus takes a different perspective. We help the organizations uncover what those root issues are and to focus their resources, that is not just people, it is money and tools as well as their energies within the organization and to those areas of their enterprise that are going to be effective. Focusing on reduction of actual business risk. To put it all together, if an organization wants to truly understand where they are in their cybersecurity maturation process, identify their gaps, measure their business risks, and to apply focus specifically on reducing business risk and potential impact as well as improving their cybersecurity culture, Cyturus is the answer.

CYTURUS