IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

In Conversation

In Conversation with Jake Olcott

Carol Baker

Jake Olcott, Vice President of Government Affairs at BitSight, delves deeper into the results of its latest BitSight/Forrester research and discusses the evolving role of cyber risk and its impact on an organization's revenue.

Jake Olcott is Vice President of Government Affairs at BitSight (https://www.bitsight.com), where he helps organizations benchmark their cybersecurity programs using quantitative metrics.

He speaks and writes about the role of directors, officers and executives in cyber-risk management. His paper, "The Board's Role in Cybersecurity," was published in 2014 by the Conference Board.

Jake is also a member of the Conference Board's Cyber Governance Advisory Group. He served as Cybersecurity Attorney to the Senate Commerce Committee and House Homeland Security Committee.

He is an Adjunct Professor at Georgetown University, and holds degrees from the University of Texas at Austin and the University of Virginia School of Law.

Q. You have a very interesting background. Tell us more about your work serving as legal advisor to the Senate, and Counsel to the House of Representatives.

A. I spent seven years during the legislative branch, working for five years for the House of Representatives Homeland Security committee, and a further two years for the Senate Commerce Congress committee. During this time, I was working on cybersecurity, legal and policy issues, and was responsible for bringing and managing investigations into the cybersecurity issues affecting critical infrastructure such as electric grids, cybersecurity issues, espionage, intellectual property issues, and exposures to investors.

It was a fascinating role which saw me responsible for writing legislation, and back in 2011 there was an effort that would have codified a number of different cybersecurity requirements for the government and the commercial space. I am very pleased to have been part of that, and being able to meet with such a range of people (from different backgrounds) at the Senate has clearly shaped my work.

Of course, 15 years ago there were a far smaller number of people working on cybersecurity issues compared to today, but one of the things that I started to notice was that we had a tendency in government to treat cybersecurity as a classified issue.

A lot of conversations about cyber breaches were all happening in a classified setting. I started to come to some conclusions that we needed to become more transparent about the problem because it was not going to be solved in a classified setting.

It's partly what drew me to the idea of cybersecurity ratings, and BitSight was also feeling this need to make these issues more transparent in the marketplace, so that the market could start to address and solve some of these problems, as opposed to just talking about them behind closed doors.

Q. The latest BitSight/Forrester's report, *Better Security and Business Outcomes with Security Performance Management – mitigating risk and generating revenue with metrics that matter* (https://info.bitsight.com/forrester-study-security-performance-management) **highlights that it is "time to manage your security like a business". When you were working with Forrester on the report did you find that this was a particular point that BitSight wanted to get across or was it Forrester who were driving the focus?**

A. That is a good question. I would say that it was driven by both. First, this has been an issue that has been very important for BitSight to explore, and we have been involved in a lot of these conversations. Not only do organizations use security ratings to better understand their own security performance, but also to better understand the security of their business partners, their vendors, and contractors, etc.

What we could see happening was that an organization would be looking analyzing the security ratings of third-parties with whom their business partners were dealing with, and sharing that information with their business partner.

If the rating was a strong rating, the business partner was really able to use that to their advantage, because they are then able to demonstrate that they were performing well when it came to cybersecurity. This provides evidence that you can trust us in our business relationship. We saw this clearly from a market perspective.

Secondly, one of the other reasons we wanted to work with Forrester was that Jeff Pollard, Vice President, Principal Analyst Serving Security & Risk Professionals had recently carried out research into the idea of *Security for Profit* (https://www.forrester.com/report/Security+For+Profit/-/E-RES151377). In the research, Pollard was able to show that organizations who are able to

demonstrate strong security practices are able to drive more revenue.
It was Pollard's piece of research that led us to work with Forrester on our latest research *Better Security and Business Outcomes with Security Performance Management – Mitigating risk and generating revenue with metrics that matter* (https://info.bitsight.com/forrester-study-security-performance-management).

Pollard had spent a lot of time talking about the metrics and measurements which security leaders should be leveraging as part of their board level report – so this was an analyst who had pretty much tapped into board level conversation, and therefore was able to bring a great deal of insight into the BitSight/Forrester report.

Q. In your research you talk about "cybersecurity risk ratings emerging as an early security measurement bright spot … with 45% of companies using cybersecurity ratings". As this is nearly half of businesses surveyed, have you seen a massive take up of cybersecurity risk reports?

A. That is a very interesting question. What I would tell you is that we have done a number of surveys this year, and we have found that 45% is consistently quoted.

Earlier in the year we worked with the Centre for Financial Professionals (CeFPro), and although the research was primarily focused on the financial sector, the number responded who were also using security rates was also in the 40-50% range.

Over the years, we have seen a significant adoption in cybersecurity risk reports, particularly among larger enterprises, but this is now filtering down to smaller businesses.

Q. Your research findings also found that "more than one third of companies agreed that they have lost business due to either a real or perceived lack of security rigour". Could you explain more about this?

A. We all understand losing business because of a real lack of security performance, but a perceived security risk can also lose a business revenue**.**

For instance, a perceived security risk could occur when the way you are presenting information differs from the way that is being perceived – either by what you are telling me, or whether it's through a security rating. I find that really interesting, and it is clear that when we don't have enough information, or how the information is being presented – has a major impact on the ability to understand the situation.

Q. There is a particularly interesting graphic on page 11 of the report that looks at how "companies seeking advanced metrics are more mature". Can you explain more about this?

A. I know **IT for CEOs & CFOs** covers the relationship between technology leaders and executives at board level, and what we have seen over the years is certainly an evolution in the way that a board member perceives their responsibilities in participating in the cyber risk discussion. Board members are feeling increasingly responsible for the oversight of cyber risk, but they are challenged by the information and data being shared with them by CISOs on the business**.**

Again, there have been a lot of studies which have been released such as Gartner, Forrester and others which have highlighted the gap between what a board member understands what is being reported from the CISO.

Board members have said time, and time again, they do not understand what the CISO is telling them, so the idea of metrics and measurements are important in understanding our own organizational security performance. But they play a very critical role in being able to communicate this throughout the supply chain.

Q. Is there anything else that you would like to get in front of our readers?

A. A: All our research is showing that whilst 40% of organizations are currently using security ratings, 30% don't appreciate the value of security ratings**.**

There have still been too many breaches in recent years which have highlighted that board members need to be very much attuned to cyber risk and the importance that they participate in this conversation.

But then the question turns to, "How should we be measuring and managing this risk?" "What should our organization be sharing up the chain?"

I think what is interesting about our latest research is that is actually highlights the fact that security does not have to be just a risk issue.

There are benefits – clear benefits – in organizations investing and appropriately managing and measuring their own security performance, the organization is able to demonstrate to its investors, regulators, and business partners that it is a better risk than its peers. It can be trusted to better secure your information and your data – and this can really drive business opportunities.

The notion is changing that cyber security is just a place – a cost centre – to one of security as a market differentiator and that is a very interesting space for organization to be.