counterparty, and the risk that they have business interruptions problems in the future, and therefore represent a credit risk.

So, I am seeing some interesting ESG perspectives coming from the credit risk bucket. Scott Davis is senior coordinator for our credit initiative. Scott, do you want to add anything to that?

Scott Davis:

Yeah, I agree.

It can be very difficult to get your hands on, but from credit risk perspective ESG can bring an interesting view into risk. Consider the recent colonial pipeline incident, was that not a “governance” thing for ESG? Poor governance over Cyber vulnerabilities could be thought of as endangering counterparties, vendors, even the customer public. If I am a counterparty to Colonial, and I rely on them for my products, I care about their cyber practices. How should we think about and measure cyber risk management processes found at my key vendors? Weaknesses in governance over their internal cyber risks is my risk as well.

I guess I would ask Mike, would you consider cyber security in this vein? Is it something you would put into ESG, or is this something outside of that?

Mike Prokop:

I actually think cyber is related to ESG, and I see that in a lot of different ways.

First of all, it’s interesting you bring up the data. It all comes down to data. You know me, I'm a data guy, so I see ESG depends on data. This is social data, it is environmental data, it is also market data. And cyber security always comes into play here, right? Because there are real dangers that you could have data corruption, data theft, data kidnapping held for ransom. In that respect, cyber always has to be considered.

Bob, you mentioned something that boards are talking about a lot these days. I can tell you that with high-profile incidents like Colonial, Solar Winds, the food processing group, and others that have experienced cyber-attacks, this topic has really taken over. Cyber is huge for everybody in all industries it seems right now.

And Scott, you bring up a good point, there is no reason why ESG and cyber shouldn't be talked about hand in hand. At CCRO meetings and with customers of Alliance Risk we have talked about integrated risk management. At the Alpha Insight Canadian conference [video link], we spoke about “four pillars”. Which was ESG, risk management, risk resilience, and digital transformation. All of those within a corporation have to be interrelated. It’s all about awareness, all silos have to be broken down and those four areas have to work very closely together because they are so interrelated.

ESG is getting that seat at the risk management table now. Good point. Good old business disruption risk analytics, right Scott?

Scott Davis:

That's right, Mike.

Participant:

Quickly, we can say these current financial industry standards don't even work if you are going to target energy...

Participant:

Here is something interesting to consider; "second order effects". So, let's say that as a company you've decided you are going to have a really strong adherence to certain ESG policies, are going to require that counterparties do the same. You're not going to go buy oil from somebody if they are doing things I don't like. Then at some point in the future you discover that a counterparty is doing something you don't like. Well, suppose that counterparty involves a five million barrel hedge position that has been on the books for 20 years. Getting rid of that hedge and replacing it to comply with your ESG policy... well, it could be very difficult to replace that position, right? So, there is a very real risk related "second-order effects" or cascading risks that must be considered.

Mike Prokop:

Right! I think that goes back to what we mentioned earlier about "integrated risk management." The silos have to be broken down. If your ESG guys aren't talking to your risk guys, well, these second-order effects can be completely missed. They could easily not appreciate the internal risk ramifications of their actions.

Mike Deluca.:

I would like to go back to Krishnan's earlier point on the baby steps. I see codifying a framework for effective cyber risk policy [a "G" component] as one such baby step opportunity for CCRO.

So, as you guys know not every company is global and/or public. Many of our mid-size or small customers have very little knowledge of ESG. So, the baby steps that we have been taking during recent years involves conducting some due diligence beyond financial statements as it relates mainly to cyber security. We started with business interruption, hurricanes and things of that nature. But today, more prevalent are the cyber security questions. True, there's not an accepted framework for best cyber risk policies yet.

So, identifying effective cyber risk management standards is an area I hope the CCRO will be delving into here.

But for now, we have to make do with just seeing if customers are thinking about cyber risks.

I put a lot of weight into the robustness of the management team. And the list of cyber risks they were thinking about. Not everyone has the cyber resources of a large major energy company, and I get that, but at least all should know that cyber risk is present for them. And so, this is an example of a baby step that we have been taking from our risk management standpoint.

Roderick Austin:

Does that fit into something like a credit risk KYC process?

Mike Deluca

No, it is more from an assessment standpoint. It is primarily involved in our credit discussions with the finance folks or the CFOs. Especially those where we have structured transactions. There, both of us have a lot more skin in the game. We want to figure out where a company might get tripped-up and experience adverse effects on their credit reserve or operational issues.

Scott Davis:

Yes, I agree.

A benchmark-able cyber risk framework is a good example of an ESG baby-step area for the CCRO, to advance energy company practices on the governance side of ESG.

One of the things that Mike Deluca and I are personally trying to help the CCRO do is find third parties that we could partner with, to leverage some existing framework standard or metrics that look at cyber security voracity, or effectiveness. I don't think we want to reinvent the wheel here. I believe Bob is working now to flesh some of this out, at this point it is just a discussion. But I agree this is a path we should be thinking about.

Bob Anderson:

Agreed, cyber seems to me to be an example where the CCRO could get immediate traction.

I should mention Paul Turner shared a really good insight with me yesterday. When I was talking to him about the CCRO ESG initiative and concerns about how dauntingly broad ESG challenges are across all industries. Paul said,

"Well, it sounds to me like if we can find places where the energy industry is either uniquely or disproportionately impacted by ESG, that is where the CCRO should be."

That way he suggests CCRO can be sure to be bringing unique value to the energy industry and all stakeholders.

As we are evaluating possible baby steps, I can further suggest;

we should look for company functions that are both squarely in the risk space and that are significantly impacted by ESG transition.

One such function that is squarely in the risk space, is credit. These cyber suggestions seem to me to be all about advancing credit assessments to include ESG.

Morgan Davies

You know, we conducted CCRO survey interviews on ESG with most CCRO members earlier this year. The results showed that cyber is top on the minds of risk officers when thinking about risk resilience. Since Colonial happened, I now I see cyber security considerations all over the place, even at larger companies, right?

I also agree that cyber may be a good choice for CCRO traction in the “G” of the ESG space.

Bob Anderson:

Also in the vein of assessing third party ESG performance as part of a credit assessment, ratings come to mind. It seems everybody wants to understand better how ESG ratings are being calculated, or otherwise assessed. We may be able to have one or more of the rating agencies become part of our ESG initiative. Our CCRO work could have some influence on methodology or what data is communicated to support the ESG rating assessment, with the goal of increasing consistency.

I'm thinking this is similar to our original work on price reporting practices. Back in the day, CCRO published best practices for price reporting at a time when the industry had lost confidence in how publishers determined market prices. Price reporting standards were needed by industry then, much like with ESG ratings today.

Maybe there is a baby step example here for the CCRO to bring clarity and consistency to ESG rating methodologies and data?