Fraud Protection & Compliance
Cybersecurity

QUESTION & ANSWER

Managing Third-Party Cybersecurity Risk: New Tools and Best Practices

Doug Clare

Vice President, Fraud, Compliance, and Security Solutions

Executive in charge of FICO's Cybersecurity, Fraud, and Compliance product portfolios, with decades of experience in risk management, advanced analytics, and quantitative tools for fraud and compliance management.

Twitter @dougoclare

Vincent Voci

Cyber Policy Director, U.S. Chamber of Commerce

Director in the U.S. Chamber's Cyber, Intelligence, and Security Division, supporting advocacy across issues that include national security, cybersecurity, and global supply chain.

Twitter@VinceVoci

"The U.S. Chamber's Assessment of Business Cybersecurity and the FICO® Cyber Risk Score allow companies to evaluate cyber risk from the outside, giving them the tools they need to start a more meaningful dialogue with partners and suppliers."

Doug Clare, Vice President, Fraud, Compliance, and Security Solutions

FICO

Presented by the U.S. Chamber of Commerce and powered by FICO technology, the **Assessment of Business Cyber Risk (ABC)** provides an empirical measure of the aggregate cybersecurity risk faced by the U.S. business community. As such, the ABC offers an easy-to-understand key performance indicator for navigating the complex topic of cyber risk. Businesses can better understand how their unique risk profile stacks up against relevant peer groups and similarly situated organizations. In this conversation, Doug Clare and Vince Voci discuss why the ABC, and the **FICO® Cyber Risk Score** for individual companies, have become important tools in helping businesses of all sizes to better align security resources and investments.

Q: How does the ABC help non-IT executives to understand cyber risk?

Vince: Cybersecurity is a top priority for the Chamber and our member businesses. Organizations must manage or transfer risk, but gone are the days of ignoring cybersecurity. That's why we partnered with FICO; the Chamber is seeking to create opportunities for improved knowledge sharing and richer discussions between, and within, organizations and with business partners.

Our report brings a quantitative assessment of breach risk to what has been a qualitative discussion. The ABC's national risk score offers an instant, point-in-time understanding of cyber risk across the broader American business community.

But the national risk score is just the starting point. Businesses need to know their own cyber risk levels and that's why the Chamber also encourages businesses to subscribe to the FICO® Cyber Risk Score, which provides scores for individual organizations and

is available at no cost. If you review the ABC and subscribe to FICO's Cyber Risk Score, your executives will have a deeper understanding of not only your firm's position relative to the national score, but also a cohort of similarly situated organizations, for example, similarly sized or serving the same vertical market.

Together, the ABC and Cyber Risk Score give organizations a point-in-time snapshot of comparative risk. Over time, you can see how risk is improving, or not, and how it continues to relate to the risk performance of a national cohort.

Doug: I agree with all that. I think that the Chamber has done a great job in starting a dialogue about cyber risk and getting people to talk about it. That applies to its work with FICO and the ABC, but also all of the other conversations the Chamber convenes between government and the private sector. They do this in Washington, and also take the show on the road, bringing organizations of all sizes and types into the dialogue.

Big organizations have invested a lot in understanding cyber risk and addressing cyber challenges. Some small and mid-size ones need a nudge to make sure they're tuned into this rapidly evolving risk.

The Chamber has tremendous resources to bring people together and start a cybersecurity conversation that people can take back to their office and figure out who they should be talking to. The ABC, coupled with the work the Chamber does more broadly, has helped organizations recognize they need to spend more time thinking about how to address cyber risk.

Beyond that, the Chamber has also done a great job of getting companies to think about not just their own security, but also the companies they're doing business with—which in many respects is even more important.

Q: Why is it important for companies to have some level of understanding about their business partners' security posture?

Doug: Companies frequently have no idea about the security of their business partners. Large organizations and regulated ones tend to have a good handle on it, but small and medium sized firms are just coming to grips with the significance of this type of vulnerability.

All companies need to understand third-party cyber risk in terms of their own supply chain, and their role in their customers' supply chains. The ABC and the FICO® Cyber Risk Score allow companies to evaluate cyber risk from the outside, giving them the tools they need to start a more meaningful dialogue with partners and suppliers. These tools give them an opportunity to prioritize third-party conversations and activities to focus on the most pressing needs first. All companies have limited resources, so tools that rank-order risk serve to prioritize naturally limited investment.

Here again, the Chamber's work in convening people to have conversations about third-party risk management has been very valuable.

Q:
What are the best practices the Chamber of Commerce recommends to reduce cybersecurity risk?

Vince: Our members and the broader business community are challenged with a new reality. Today, our digital economy is increasingly interconnected, making perfect security unachievable, but risk management and resilience more critical. That's why the Chamber urges organizations to understand their risk, manage it, and then find a risk transfer mechanism, such as cyber insurance, to help offset the risk that will naturally remain. This cycle of ***measure, remediate, transfer*** represents a best-practice approach, allowing businesses to protect themselves and their customers responsibly and efficiently.

More specifically, one of the things I like about the in-depth report that accompanies the ABC is that we make recommendations for any organization to better understand their risk and how they can manage it. The Chamber strongly supports the **NIST framework** and would urge organizations to use it or a similar information security protocol, along with tools such as the FICO® Cyber Risk Score, to understand risk better and put in place effective risk transfer mechanisms. These are all good recommendations from our joint efforts with FICO on the ABC.

Q:
How exactly does the FICO® Cyber Risk Score help non-IT executives to improve their company's security posture?

Doug: For a long time, security has been a bit of a murky technology realm, where business leaders have assumed they should get out of the way and let the tech experts sort it out. But a few of the big breaches in recent years have become a collective watershed moment, when executives started really paying attention to the criticality of cyber defenses; they realized that cyber risk needed to be elevated to the same status as other C-level risk management concerns.

Fast forward to today's environment, and the Cyber Risk Score does a couple of things that are extremely important. First, it gives non-IT executives an understandable language for cybersecurity conversations, and the opportunity to say, "I'm good at doing X and getting better at Y than I used to be, and here's how I compare to my peers."

These are valuable inputs for budget owners to know, to help determine whether or not they're making the right cybersecurity decisions.

Second, as I mentioned earlier, the Cyber Risk Score provides insight for organizations to understand supply chain risk. Of course, it's harder to understand third-party risks in granular detail; you never get to know as much about another firm as you can know about your own.

Evaluating a third party through a scoring service doesn't get you out of doing detailed due diligence on your supply chain, but having the ability to compare Vendor A and Vendor B, and have a conversation with Vendor A about what they might need to do to reduce their risk of data breach, in between or in lieu of major audits, is a valuable benefit. It allows organizations to risk-rank suppliers and more effectively prioritize the work of their supply chain risk team. The quantitative tools support and direct the use of the qualitative tools in your risk management arsenal.

FICO has been in the risk quantification business for decades. One thing we know for sure is: What gets measured gets managed. Cyber risk management has turned into a domain where quantitative and qualitative methods match up very well.

Join national business leaders, and your own management team, in the conversation on how to reduce cyber risk. Get the U.S. Chamber of Commerce Assessment of Business Cyber Risk report and your company's free FICO® Cyber Risk Score today.

www.uschamber.com/cyber-abc#/

www.fico.com/en/products/cyber-risk-score

4794EX 01/20 PDF

FOR MORE INFORMATION
www.fico.com
www.fico.com/blogs

NORTH AMERICA
+1 888 342 6336
info@fico.com

LATIN AMERICA & CARIBBEAN
+55 11 5189 8267
LAC_info@fico.com

EUROPE, MIDDLE EAST, & AFRICA
+44 (0) 207 940 8718
emeainfo@fico.com

ASIA PACIFIC
+65 6422 7700
infoasia@fico.com