ceocfointerviews.com

Issue: April 10, 2017

CEOCFO Magazine

Cyber Strategy that Protects Valuation and Reputation

Israel Martinez
President & Chief Executive Officer

Axon Global
www.axoncyber.com

Contact:
Israel Martinez
(202) 248-5050
israelm@AxonCyber.com

***"We deliver a simple but powerful report about what is relevant today. The report details those active exploits that may affect your valuation and reputation in a way that impacts the board."*- Israel Martinez**

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: ***Mr. Martinez, would you tell us about Axon Global?***
Mr. Martinez: We specialize in Cyber Enterprise Risk Management and Governance. We are certified experts that understand how to reduce or eliminate the liability of cyber risks that can impact valuation and reputation. We are recognized as leaders in our field by the U.S. Secret Service and by the Department of Homeland Security.

CEOCFO: ***What are some of the differences you might be looking for when you are helping a person in that category?***
Mr. Martinez: We are looking for executives who are genuinely interested in understanding the cyber security risk posture of their company. Cyber security is often seen as a technology problem. We believe it is more of a governance and a risk management problem. If you have board members asking the right questions, then you get the C-suite to focus on the right policies and incentives. For example, recently the FCC started a criminal investigation at Yahoo!, as it relates to behavior surrounding cyber security breaches and compromises. An appropriate question for board members is whether they have had similar behaviors. Executives are quickly learning that it is usually not the event (breach), that is the most expensive or that introduces the most liability for the corporation. It is the behavior around that event that can get expensive. If you do not have the right policies in place, the right responses and "tone at the top", regarding the incident, then you will have bigger liability issues than just the cost of the breach. See: https://axoncyber.com/faqs/

CEOCFO: ***Are people understanding the depth of the problem as far as liability as opposed to the technology?***
Mr. Martinez: I think they are understanding it but they are not understanding what to do about it. If you look at the National Association of Corporate Directors (NACD ®), that is the largest association of board members in the world. I'm a full board member and faculty for them and I've seen they have done a very good job in terms of explaining that risk management is now a board level issue. What is not clear, is what to do about cyber security in terms of avoiding the threat or the liability. I think that is where the focus is beginning to shift, for companies like ours that advise on the cyber risk mitigation strategy. Some of the answer is in technology but a lot of it is determining what is a reasonable standard for policies, communication, protecting data, intellectual property and most importantly protecting the valuation and the reputations of the people and brand. The answers about how to mitigate these risks are just now evolving in the marketplace. See: https://axoncyber.com/fyi/

CEOCFO: ***Would you walk us through a typical engagement?***
Mr. Martinez: The biggest compelling event in the marketplace for Axon Global is that the SEC recently announced that corporations need understand their supplier risk profile. Everyday corporations electronically engage suppliers and the reality is that some of those suppliers, especially in the small to medium sized enterprises, are already infected with some

type of espionage, ransom-ware or cyber threat and pose a risk. We as CIOs and CISOs traditionally focus on securing the perimeter of our organization. When you look at your supply chain, many of those are integrated into the system from the outside into our networks. There is now a requirement to inspect those suppliers and determine which are perhaps unknowingly polluting our organization. Axon is able to report those without "touching" the network of our client or of their supplier. Our typical engagements are about answering which of the 3rd parties represent a substantial risk. We answer that question quickly and effectively with no required hardware/software or contracts to sign. See: https://axoncyber.com/services/

CEOCFO: ***How are you able to do that?***
Mr. Martinez: We use artificial intelligence in how we search the deep web for bad actors actively exploiting the client. Most companies are looking inside of a network for where malicious activity. We focus outside of the organization network, on the bad actors in the deep web. We have a complex matrix of contracts with the United States government, with international governments and also with the private sector clients that allow us to legally search the deep web to acquire that information (what bad actors know and exploit about our clients). We then bring that knowledge and evidence back to the client in the form of a discreet report. We discuss it in business terms explaining what has happened, whether it is still happening and how they can stop those nefarious activities quickly, with their current resources. We deal with what is called extreme actionable information. Those are things that are happening right now that the organization does not know about. This empowers our clients to optimize allocation of resources immediately, and to eliminate or mitigate these risks, before a breach occurs.

CEOCFO: ***Would you tell us a little about the dark web; how it works and how you are able to access what you need to achieve results?***
Mr. Martinez: If you imagine an iceberg, 10% of an iceberg is what you see above the oceans' surface but 90% of it is underneath and thus dangerously deceptive. The internet is the same way. What we experience each day in terms of commerce, social media and all other applications, represents about 10% of the internet experience. The other 90% is what we call the deep web. It is in that ecosystem that bad actors live and exploit using tools like TOR, a browser which disguises who they are and where they are, effectively disguising nefarious transactions. If you can imagine showing up at a costume party where everyone wears a mask – you don't know whose those people are. Yet, these characters are able to conduct illegal transactions with each other, everything from buying and selling drugs to human trafficking without revealing identities. They are able to do it in a way that is very secure and very difficult for law enforcement and the government to identify these individuals. The internet was never meant to be forensically accurate so it is conducive to having these costume parties if you will, where people are exchanging illegal information, money and other things of value in a way where they are rarely caught. We have spent decades understanding the secret handshakes in this environment and then automating tools that hunt, track and retrieve relevant information about threat actors, exploits and compromises.

CEOCFO: ***Why is it that companies cannot have that same level of security?***
Mr. Martinez: The answer goes back to the compelling event for our business and that is, is the uniqueness of the supply chain affecting you. You can do everything right in an organization - imagine securing your home where you have locks on doors and windows but then you accidentally invite what we call a bad actor - people who have mal-intent. The same things happen with our networks. We have to be very careful with not just securing our environment but who invite to integrate as partners or suppliers. We must insure they are practicing proper "cyber-hygiene" in a way that allows them to interface with us securely. It only takes one or two suppliers infected with espionage for example, to pollute our networks. Most cyber criminals focus on the easy targets like small to medium businesses that do not have the resources to secure their environments. They hijack credentials of people in that group that are suppliers to Fortune 500, Fortune 1000, or perhaps suppliers to the government. This was they come in through the back door into a well protected large company. Bad actors have lots of time to plan and are always looking for the easiest path to a successful breach.

CEOCFO: ***Do you work with your clients on an ongoing basis or do you set up a program they take it from there?***
Mr. Martinez: We can do both, we make it easy to engage with us. We deliver a simple but powerful report about what is relevant today. The report details those active exploits that may affect your valuation and reputation in a way that impacts the board. The client can then use the report to allocate their own resources to mitigate the risk, that's a simple two hour engagement. These reports identify exploits that are usually time-sensitive, if the client acts soon, then the risk can be eliminate or mitigated. We deal only with extreme issues, for example, halting the theft of sensitive intellectual property. There are plenty of malware companies out there that stop smaller-grade infections. But answering the Governance questions requires unique experience and skills, which can take several advisory sessions with the executive team. For example, today companies have an obligation if personal information is stolen to report it to the public or their

shareholder. This would have valuation and reputational implications. We help boards answer those questions in as little as a one hour session or via advisory engagements that can last months. Another example, if intellectual property is stolen, there is really no clear mandate about reporting to shareholders or to other stakeholders. How will you decide as an executive whether to report or to whom? The timetable depends on the complexity. M&As are usually quick engagements (days). However, if you are going through an acquisition and management knows your intellectual property has been stolen by a nation-state, disclosure becomes a tricky proposition. This is another area where engagements can vary from a few hours to several weeks. Most of the time, we can report findings within a few hours - without touching that network – and do a quick hand-off to the C-suite.

CEOCFO: ***Are you working with government agencies as well?***
Mr. Martinez: We are. As I mentioned we have a complex matrix of legal contracts, that allow us to track bad actors, and to monitor them in a way that is within US and/or international law for the private sector and for United States government. Our clients range from F500, through mid-market companies across all industries and government such as the Department of Homeland Security and the Defense Information Systems Agency.

CEOCFO: ***What would you like to be able to do or do more easily in helping companies?***
Mr. Martinez: I think there is a great program with the Department of Homeland Security. These are called Information Sharing and Analysis Organizations (ISAO). These ISAOs are government-private sector non-profit cooperatives that are allowed to share information about cyber threats without liability. Think of a "neighborhood watch program", but it is in cyber. These ISAOs are able to execute cyber "if you see something, say something" programs that allow for sharing of cyber threats. As an equivalent example; knowing how someone broke into a home last week can help a neighbor prepare and protect against that recent attack. When ISAO members share that information the Cybersecurity Act of 2015 declares a release of liability for sharing it in accordance with the ISAO standards. What would be great is if there was a national program to educate general counsels that this program is available. Today most general counsels go out of the way to not receive active exploit information about their respective company for fear of liability. However, they are glad to receive it about their suppliers. This dynamic has to change.

CEOCFO: ***How do you reach out to potential clients and how do people find you?***
Mr. Martinez: We are a specialty group, so most of clients find us through associations like the American University Kogod Cyber Governance Center or groups like NACD or the Association of Corporate Growth (ACG) -which is one of the largest associations of non-public stakeholders in mid-market companies. You can find us at AxonCyber.com