DRAGOS
SAFEGUARDING CIVILIZATION

YEAR IN REVIEW

LESSONS LEARNED FROM BOARD OF DIRECTORS BRIEFINGS

2018

INSIGHTS TO BUILD AN EFFECTIVE INDUSTRIAL CYBERSECURITY STRATEGY FOR YOUR ORGANIZATION

Over the last year, I was an invited guest at around a dozen board of directors meetings of forward-leaning energy and manufacturing companies in the United States. As a guest of these boards, I was asked to brief on the industrial cyber threat landscape, including industrial control systems (ICS) networks. The questions from the boards were almost identical between every organization, even though the organizations' sizes, geographies, and focuses ranged greatly. The purpose of this paper is to share common questions and concerns from the various industrial organizations I briefed and the responses I gave to help organizations build the right industrial cybersecurity strategy.

—

Robert M. Lee
CEO and Founder of Dragos, Inc

BOARD LEVEL QUESTIONS

HOW DO WE KNOW IF WE'RE UNDERSPENDING OR OVERSPENDING ON ICS CYBERSECURITY?

WHAT IS THE BEST THING WE CAN DO TO GET STARTED THAT WILL HELP MOVE US FORWARD?

IF A MAJOR ATTACK HAPPENS, WHAT IS THE ROLE OF THE GOVERNMENT?

Board Level Questions

A board is a unique group of people who guide companies and manage risks to it. When the boards expressed curiosity about the cyber risks to their organizations' industrial and operations networks, the questions raised were surprisingly similar:

- ***How do we know if we're underspending or overspending on ICS cybersecurity?***
- ***What is the best thing we can do to get started that will help move us forward?***
- ***If a major attack happens, what is the role of the government?***

These questions are very reasonable board level questions, and I was impressed with the maturity levels of the boards and their understanding of cybersecurity, as well as their appreciation of its complexity. I had a feeling these boards constantly met with "experts" who advised them of "best practices," which left them with analysis paralysis at the competing guidance. To these questions, my responses were consistent for each company.

How do we know if we're underspending or overspending on cybersecurity?

Almost universally, my response was that it was very likely the organization was underspending on cybersecurity related to industrial and operations networks, because these environments have largely not been considered part of the cybersecurity strategy. Threats are increasing in frequency and impact, but they have existed for a long time without being identified, due to a lack of visibility into these networks and the threat landscape. Most risks to organizations are on the operations side of the house (where they generate money), not on the enterprise side, where they may interact with most employees and customers. I consistently noted that most organizations have spending flipped between their enterprise networks and operations networks in terms of where the risk is and how they are managing it. This is not to say that enterprise network security should receive less focus or funding, but instead, it is a realization that not a lot has been done before in industrial networks besides forcing segmentation and separation that often does not last.

However, my answer of underspending was only the beginning. It is just as easy to start overspending once organizations realize the risks exist. To each board, I recommended they ask their executives and security personnel to identify the top scenarios that would introduce significant risk to the company from cyber threats. In industries where there have been major attacks, such as the Ukraine 2015 and Ukraine 2016 electric grid cyber attacks, those attacks should constitute the first scenarios. The board should then ask: if those attacks were to happen, how would we fare? I explained that taking an intelligence-driven approach to security provides a ground truth reality of what is really happening instead of just theoretical topics.

By gaining an understanding of the scenarios that would introduce the most risk and agreeing on them at the board level (especially in regards to attacks that have already taken place), boards are effectively giving guidance that can be turned into actionable requirements for security teams. I ended this response to the boards by noting they should demand that cybersecurity strategies contain protection, detection, and response capabilities--each with well-trained and empowered defenders. Simply relying on protection as a preventive function would, and has, consistently failed.

What is the best thing we can do to get started that will help us move forward?

This question is a reasonable call-to-action. It can feel very frustrating and powerless not participating in the resolution of the concerns the boards have articulated. In many cases, I had the distinct impression many of the boards were heavily invested in cybersecurity, but had not received the reassurance their security teams were prepared. This can lead to uncertainty and an overreaction to hype that so commonly occurs in our industry, such as news headlines that misunderstand cyber attacks to infrastructure; therefore, the first action to get started, in my opinion, must include a component that includes the board of directors (which links to the first question of underspending versus overspending on cybersecurity).

It is my recommendation that boards should ask their security teams to create a tabletop exercise that includes the board of directors at some point. If a tabletop exercise has never been performed for industrial networks, there should be one without the board first. The exercise should be based off one of the scenarios the board has agreed introduces significant risk to the organization, and if possible, should be based off one of the real attacks that took place; for example, oil and gas companies could base a tabletop exercises off the 2017 TRISIS attack in Saudi Arabia. Electric companies could use the 2016 CRASHOVERRIDE attack in Ukraine. Manufacturing companies could use a ransomware worm outbreak, such as WannaCry.

Tabletop exercises are more valuable when paired with technical assessments. As an example, security teams could perform threat hunts in their environments to look for one of the threats they've identified as an important scenario, and as a result, better understand their current protection, detection, and response capabilities. Those findings could then be used to model the tabletop exercise off of; additionally, they should include security and operations staff. Once one tabletop exercise is complete, the board should be included using a different scenario. If there is only one real-world example security staff can model the exercise on (though there are numerous for each industry), the real-world based scenarios should be presented to the board. Tabletop exercises should include a focus on understanding compliance, risk, and legal challenges, as well as a major focus on communication across the executive teams, effective communication throughout the organization, and what their communication strategy is to customers and external parties such as the government.

Tabletop exercises give comfort to boards, while highlighting direct and tangible requirements to improve security across protection, detection, and response capabilities in organizations' industrial networks. These exercises also provide visibility of gaps worthy of funding and clearly map to the question of underspending versus overspending on industrial cybersecurity strategies.

If a major attack happens, what is the role of government?

Critical infrastructure asset owners and operators are keenly aware that a response to any major cyber attack will include the government at some point. When thinking of communication strategies to external parties, it is common to question the legal requirements that exist as well as proactive communication that would be beneficial. I was surprised that almost all of the boards I briefed were already aware that there would be no ability for any government agency or team to swoop in and save the day. They understood security relied on their organizations and that the government's role was different.

However, each board also expressed confusion about the role of government, because representatives of different government agencies had briefed them in the past and left them with competing answers of whom they were suppose to call. Members from the Department of Homeland Security, Federal Bureau of Investigations, Department of Defense (especially noting the National Guard), and Department of Energy all had similar, if not identical, messages focused around: "call us first." When the boards asked my opinion, I noted that each government agency has a role to play and are actively finding routes to work together amongst themselves. I called special attention to the Department of Energy's Cybersecurity, Energy Security, and Emergency Response (CESER) and Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) as two agencies I am currently optimistic about in terms of how they are viewing the problem and their roles to help private sector. Each government agency head can often clearly articulate how they work together, but the representatives that go out into the field and talk with companies often have competing narratives that I suspect are tied to how they are measured. As an example, it is common knowledge among security teams of infrastructure companies that holding security clearances does little for them in terms of defensive insights and recommendations, but representatives of government agencies push companies to get security clearances so aggressively that people assume they are being measured on how many companies have been engaged and moved forward in the process.

My consistent message to board members was that each government agency has a role, but they should be prepared to have a point of contact at each government agency they want to communicate to and ensure communication is done in writing. It is extremely easy, especially in tense situations, for verbal communications to be taken out of context or misheard. Additionally, I noted that in most cases, contacting the government--unless it's a requirement--is best left until after the incident is well understood and the security team has a handle on the direction moving forward. Including additional outside parties besides teams that have rehearsed to be there, such as an outsourced incident response team, always introduces complications and adds complexities such as communication--and, potentially, leaks. At some point, the inclusion of the government will add value, but be sure to rehearse and understand when it is appropriate to bring them into the conversation, which relates back to the value of tabletop exercises.

CLOSING THOUGHTS AND RECOMMENDATIONS

In addition to spending time with boards of directors, I was often afforded time to get to know the security teams and the Chief Information Security Officers of these industrial organizations. The same briefing I gave to the board of directors, I would share with those security teams, highlighting different points, as well as what their boards were asking. I found those teams often significantly appreciated insight into the boards' thought processes. There was also a very common concern across these teams that the existing security organization, primarily focused on enterprise security, was going to be asked to address industrial security with little to no increases in budget, personnel, and training. This is a very astute concern.

It is imperative that organizations understand increased investment will be required especially in areas of people, processes, and technology. The board level concerns common between these organizations show an appreciation of this, and when resource increases are tied to those concerns, it will be easier to keep organizations on the same page–top to bottom–about requirements and the appropriate level of spending. I have long advocated that security operations are vital to countering threats. Simply deploying passive defenses or security technology and keeping them tuned will reduce noise and some cyber risk to incidental malware outbreaks, but this will never provide the insight and feedback loop required for security personnel to counter targeted threats. The focus of human defenders taking a proactive approach to countering human threats inside their networks is called an active defense and is required. Most organizations have focused on architecture issues and maybe passive defenses–though often not industrial specific–and rarely, if ever, enable a truly active defense.

In the next year, I challenge organizations to look at their investment into industrial and operations networks and ensure that it is not only appropriate for their risks, but also done with an understanding of the threat landscape. Seek top to bottom understanding of requirements in the organization, and utilize tools such as threat hunting and tabletop exercises to bring together security and operations teams. Do not expect the enterprise security team to be able to stretch even thinner to cover a mission that, in many ways, is more challenging than traditional enterprise security without adding new resources to their efforts.