White Paper:

Understanding the company's current Cybersecurity Program: Four Key Questions

Abstract

According to a 2015 survey by EY, only 7% of senior management reported satisfaction with their own organization's cybersecurity policy. Similar levels of discomfort persist in terms of cybersecurity strategy. In a recent cybersecurity conference for board members, sessions focused on starting cyber-risk oversight efforts from the basis of strategy, helping directors take a more holistic approach to building a cyber-risk aware culture, and examining the board's ability to gain transparent communication and understanding of both triumphs and failures in the cybersecurity program. How do we know that we are making progress in these pressing areas? Based on the dynamics in these areas that we experience with clients, we identify four key questions that can help clients get a grasp on how progress may be proceeding toward getting a more fully informed oversight of cybersecurity for the board and senior management.

1) Are time and resources focused on specific point solutions, at the expense of a coherent and strategic cybersecurity program?

   At the 2016 RSA conference in March, there was a very active pattern of buyers on the exhibit floor, with attendees consistently reporting that a high amount of solution deals took place right at the show. Corporate customers were seeking out a series of very specific point solutions to fill gaps in their current set of solutions.

   If we consider the typical company and its set of cybersecurity solutions and capabilities, it can be viewed as a portfolio. Like an investment portfolio, the cybersecurity portfolio should provide us with diversification - in this case diversification in our defensive capabilities. And much like diversification in the equity markets, we value a diversified portfolio in large measure because it lowers risk, and mitigates our exposure to certain negative events.

All of this sounds logically appealing. And yet a recent observation by Booz Allen calls this into question:

> *"Currently, the cyber strategy employed by many organizations is a patchwork of point solutions. And the number of individual solutions is only growing. The problem: most of these point solutions don't work together, because they weren't designed together. String together a few high assurance solutions and the result is a large, insecure system."*
>
> \- Booz Allen, 2016

Many organizations have a multitude of archaeological layers of solutions, taxing the support process and creating unpredicted interactions and inconsistent alerts and analytical results that then need to be reconciled at the human level. Much like the unanticipated interactions among multiple prescription drugs, we can easily have a situation in which each solution has a valuable role if it were to stand alone, yet together they create a compound problem that weakens the overall program.

So how do we avoid making our defenses weaker through the multi-layered effects of weakly integrated, highly specific solutions? Just as an automobile is not simply a pile of parts, our view is that we simply cannot to obtain each capability and turn it on alongside everything else we already have. In organizations with some of the most exhaustive collections of solutions, we have seen this over-arching plan and long-term roadmap of goals lacking – if not entirely absent.

What is missing in this pattern is a cohesive plan – one that utilizes a guiding architecture. A multi-year view is doubly vital, to provide a capability-oriented “compass” against which the building of new capabilities can be weighed.

2) Do cybersecurity governance measures lag behind as a priority?

While investment has proceeded in other areas, the development of meaningful cybersecurity governance has lagged. In a recent survey, EY found that only 7% of companies were satisfied with their current cybersecurity policy. And since policy is close downstream outcome of cybersecurity strategy, it is unlikely that the 93% dissatisfied at the policy level are comfortable with their strategy in light of this finding.

An effective cybersecurity governance function would of course include at minimum,

- Cybersecurity Strategy
- Cybersecurity Policy
- Capabilities Roadmap
- Target Operating Model
- Cybersecurity Incident Response Plan (CSIRP)
- Effective organizational checks and balances
- Clear and transparent communication of cybersecurity conditions and status to senior management and the board

Yet when we have regulatory pressure, coupled with the palpable need to secure broad areas of vulnerability in the organization, the tendency can be for the attention to cybersecurity strategy and cybersecurity policy to wane. Yet for our overall program to be effective, these foundational elements have to be revisited regularly to assure their ability to provide a sound foundation for the overall cybersecurity plan.

3) Do the board and senior management feel a persistent level of uncertainty and lack of insight into vital cybersecurity decisions?

In its cyber-risk handbook, the National Association of Corporate Directors (NACD) asserts that: “boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.”

While this may seem to be a description of an ideal state, it truly is essential. We’ve seen many boards today struggle with fitting cybersecurity discussion into the already packed agenda of the typical board meeting. But that may be the easier part of the issue.

What is most often missing, even in those situations where cybersecurity is given adequate time and attention at the board level, is almost always an issue of informative content that is meaningful and board-ready. Is the board being presented with trade-offs and options for the direction and strategies of cybersecurity? Are they provided an informative set of facts that are meaningful in terms of costs, risks, financial impact, capital and expense effects of various choices? Is there agreement on a valuation model for cybersecurity program choices, which can put these options into terms that the board sees and understands as they apply to other key decisions such as plant expansion, legal settlements, workforce decisions, acquisitions, etc.?

4) Are ongoing adjustments being made to reflect the expanding scope of

cybersecurity?

As practitioner CISOs and CISSPs, we can all recall the early days of our profession when the scope of information security was focused on the "glass house" of IT and primarily corporate data centers. In more recent times, the CISO has taken on many areas, out of necessity, that extend far beyond the boundaries of IT. The role of the CISO (and by extension the overall cybersecurity program in the organization) has become one that now extends well beyond the IT organization and the domain of the CIO.

Why is this? It's due to our radical adoption and deployment of digital capabilities throughout the organization – and beyond. Cybersecurity is no longer just about data security. It's about the integrity and defense of all the points of digital exposure that introduce risk to the company. And that exposure not only could come from anywhere, but it continues to spread as fast as digital technology spreads.

This means that in the typical organization of today, our cybersecurity program has to address:

- Shadow IT, including all the corporate information on informal cloud accounts, personal hard drives, flash drives that leave the office every day, well-intentioned "backups" that people keep at home and in their vehicles, etc.
- Trading partner systems, especially the vendors and third parties with whom we share sensitive information, often through their own systems that we not only do not control, but which have security standards and provisions of widely varying and unknown effectiveness
- Cloud capabilities, including those under the control of the conventional IT organization, and those initiated, managed by, and in some cases known only to certain specific departments, divisions, regions, operating units, joint ventures or other segments of the organization
- Personal technology, which can contain substantial sensitive information starting with emails, and moving around the globe as the workforce travels across borders and through a variety of minimally secure environments
- The Internet of Things, or IoT, which includes everything that is digital or communicates to something that is digital. These can be pumps, switches, vehicles, thermostats, cameras, lighting, meters, valves, door locks, etc.

In a 2016 CIO Magazine article, R. David Moon of Arx Nimbus was interviewed by Senior Writer Clint Boulton on this subject. As stated in the article, it is our belief that the overlap between conventional IT and cybersecurity is decreasing, and that organizations are requiring ongoing adjustment of the CISO and CIO roles to reflect this. (cio.com: Debate continues over where CISOs sit in the C-suite)

From our experience, the need to continuously adapt the scope of the cybersecurity program to the shifting operations of the organization very quickly extends to organization strategy. The reason for this is that cybersecurity must adapt not only to the real operational scope of today, but must “pre-adapt” by building cybersecurity capabilities that anticipate the scope of company operations on the horizon.

Almost all key strategies end up with critical cybersecurity considerations that must be incorporated as early as possible, given the cycle time it takes to build out these vital security measures. Strategies like geographical expansion, new product rollouts, and M&A transactions all include sweeping cybersecurity implications. If these are not properly incorporated into a multi-year roadmap of cybersecurity capabilities and project plans, we will find ourselves in a perpetual state of catch-up, which opens up its own set of risk exposure.

Each of these questions has many implications for today’s organization. All managers will want to more fully incorporate cybersecurity into their planning and strategy considerations. The focus of our practice at Arx Nimbus is to build the needed linkages across strategies, senior management decisions, and the cybersecurity program to advance the linkage between these critical functions and create a more effective, transparent cybersecurity program that truly protects and sustains the organization.

Arx Nimbus is a boutique management-consulting firm that gains quantified advances in cybersecurity defense, governance, compliance and risk reduction for companies and their investors. We do this by bringing combined decades of C-level Cybersecurity leadership to provide strategic and comprehensive insights to the board and senior management. We combine deep experience in defense, logistics, financial services and technology sectors with exceptional academic credentials, equipped with comprehensive standards-based quantitative methodologies.

We structure our results for companies consistent with our experience in senior management in public and private companies including the Fortune 500, all directed to provide a strategic viewpoint into the rapidly moving world of Cybersecurity, and to help management advance the effectiveness and reliable execution of the essential capabilities for protecting the digital assets of the organization.