What do the SEC, ABA, NACD and EU GDPR Authorities all agree you need to do now about Cybersecurity Risk?

Cyber risk - Warren Buffett says it's the number one threat in our world. In your business it's crucial - the risk is real, and it's all around us and growing. But how much do we know? Can I say what my total cyber risk is, in financial terms? Where would I start, to really attack my greatest sources of cyber risk?

How does management currently select the best cybersecurity options and capabilities for the organization? Often in the past, these decisions were made based on professional judgment or expert opinion. Over time, experience and litigation have caused an aversion to personal opinion as a basis for a strong cybersecurity program. Just as no modern airline would operate aircraft without adequate automation based on pilot judgement alone, so cybersecurity has proven too vital to leave exposed to the risks associated with individual judgment and expert opinion.

The US Securities and Exchange Commission (SEC) says:

"Cybersecurity risks pose grave threats to investors, our capital markets, and our country. Controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents."
(SEC Source: https://www.sec.gov/rules/interp/2018/33-10459.pdf)

But does anyone really care about these "grave threats"? There are several parties that care, and their consensus is centered on one consistent theme: We must properly understand cybersecurity risk and understand it now.

So when we're told to "identify cybersecurity risks, assess and analyze their impact on the business, evaluate the significance associated with such risks . . ." – what does that really mean? To actually accomplish this, it seems to me we would need to be able to answer several key questions:

- How do I gain actual knowledge of my own cyber security risks?
- What are my top cybersecurity risks, and what is their relative financial impact?
- What is the value of acquiring specific cybersecurity capabilities?
- How can I chronicle my efforts at risk reduction in terms that put me on my best footing for regulatory and legal preparedness?
- How can I profile probabilities of certain risk scenarios?
- What is the value to the enterprise of risk-related measures like cyber insurance?
- How do we gain common direction and agreement among senior management to confidently support a well-targeted cybersecurity program?

The American Bar Association (ABA) says:

"Risk assessments can inform decision-makers and support the risk management process by identifying: (i) relevant threats to the organization or threats directed through third party entities; (ii) vulnerabilities both internal and external to the organization; (iii) the impact (i.e., harm) to the organization and individuals that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur."
https://www.americanbar.org/publications/blt/2016/11/cyber_center.html

So, can I really get at this level of understanding today? In the past, cybersecurity risk was considered by many to be "unknown and unknowable" – even by risk professionals and insurance underwriters. Cybersecurity threats are adaptive threats, unlike fires, floods and hurricanes. Starting in 2005, we began to gain the first basic mathematical models to even properly profile this class of adaptive threats. Only recently have these quantitative techniques come into practical use, thus obsoleting historical attempts at getting at cybersecurity risk.

Getting this level of knowledge – quantitatively sound yet practical and actionable knowledge, lets us answer many of the most vexing issues in cybersecurity today. These are the fundamental issues that have limited the traditional approaches to measure – and do something about – cybersecurity risk:

1. How do you as an organization determine the relative merits of cybersecurity strategies, solutions and initiatives?
2. How do you provide the documentation and support that helps to get compliance sign-off from regulators? How is that working for you now? Do you have concerns about getting regulatory acceptance?
3. How do you decide today on how much cyber insurance to buy, where coverage should be concentrated, how to evaluate policy exclusions and what premium you should be willing to pay?
4. Do you have a means today to track the risk that is getting addressed, in financial terms, by the various cybersecurity investments, solutions and projects as they take shape?

5. Do you have all you would need if there were a major inquiry or litigation that looked at how the cybersecurity program was developed, and why certain choices were made? Would any of that come back to the professional judgment or expert opinion of certain individuals?

The National Association of Corporate Directors (NACD) says:

"Board-Management discussions about cyber risks should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance"
https://www.nacdonline.org/Store/ProductDetail.cfm?ItemNumber=10687

To get a true understanding of cybersecurity risk, we would have to be able to measure it, quantify it, and continue to analyze its origins and effects over time. The real-world business dynamics of even the average enterprise create major dynamics that produce constant change in the cybersecurity risk landscape. These include M&A activity, new systems and applications, geographic expansion, process re-engineering, outsourcing, and even new product roll-outs.

Given today's cybersecurity threats, it's simply not enough to have a reactive stance in our cybersecurity efforts and attempt to shore up the new gaps and vulnerabilities that accompany these business dynamics after the fact. We need to be able to understand these cyber risk effects in advance and properly prepare for them. Otherwise the enterprise will find its cyber protections permanently lagging and playing catch-up – and therefore permanently vulnerable.

The European Union General Data Protection Regulation (GDPR) says:

"Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk."
(EU Source: http://www.privacy-regulation.eu/en/recital-76-GDPR.htm)

Today's prevailing authorities and regulators agree – now is the time to analyze, quantify and truly understand cybersecurity risk. Get this understanding now – contact us today and get past the current unknowns of your cybersecurity risk.

Arx Nimbus - Cybersecurity Knowledge Now

Arx Nimbus is a cybersecurity risk analysis firm that gains quantified advances in cybersecurity defense, governance, compliance and risk reduction for companies and their investors. We provide the Thrivaca® quantitative SaaS cloud platform as the first financially quantified cybersecurity risk valuation solution. We provide groundbreaking innovation in cybersecurity risk software by bringing combined decades of C-level Cybersecurity leadership to provide strategic and comprehensive insights to the board and senior management.

We structure our results 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 enterprise.