The Cyber Brief is No Longer the Boring Part of a Board Meeting

Now, everyone is engaged in the cyber discussion. It encompasses insurance, liability, risk management and total cost of ownership. Cyber is no longer a technical issue, it is a business issue.
The Cyber Brief is No Longer the Boring Part of a Board Meeting

News for the geeky guys in the back room: the cyber discussion is no longer yours. It was not long ago that the Chief Information Security Officer’s (CISO) brief to the board was met with glassy eyed stares, checking of phone messages and a chance to get a fresh cup of coffee. The CISO would stand up and list the top 50 company vulnerabilities that were color coded red, yellow and green and only got questions from the one or two tech savvy people on the board.

Now everybody is engaged in the cyber discussion. It encompasses insurance, liability, risk management and total cost of ownership. Cyber is no longer a technical issue, it is a business issue.

This reality has come into focus over the past few weeks with two significant events. First, the National Institute of Standards (NIST) Cyber Security Framework (CSF) began referencing a quantitative model for calculating cyber risk in terms of dollars and cents. The value-at-risk (VaR) model, called Factor Analysis of Information Risk (FAIR), provides a method for converting the red, yellow, green charts of past discussions into financial terms that can be utilized for sound business decisions.

The second major event was the collaboration between a cyber research firm, MedSec, and a trading firm, Muddy Waters Investing, to identify security vulnerabilities in medical devices built by St. Jude Medical. When the research discovered vulnerabilities in the devices, the result was a steep drop in the stock price of St. Jude Medical. The finding occurred in the middle of acquisition proceedings with Abbott Laboratories. Additionally, with the release of the report, a class action suit was filed against St. Jude’s. Needless to say, this event went to the very core of the company value and operations.

So what are the core business elements for companies from a cyber perspective? First, and foremost, understand that cyber is a risk issue, no different than other risk issues that companies deal with every day. Granted, the underpinnings might be different, but the general thought processes are similar to natural disasters, regulatory changes and employee malfeasance. It has often been said that cyber risk is different than other risks because it is so pervasive and has direct actors trying to attack a business and, therefore, cannot be quantified. I don’t believe this, it is a risk that has some unique characteristics, but at the end of the day, the impact is measured in dollars and cents.

Cyber Insurance

In May of 2015, I wrote a paper titled “And Then the Accountants Showed Up, How the Insurance Industry Will Drive Cybersecurity.” In that paper, I predicted that there would be a major increase in the cyber insurance market and that the insurance industry would begin to affect corporate behavior in order to minimize risk, which is in the interest of the insurance companies. A year later, I got part of the prediction correct: the cyber insurance market has exploded, with estimates of $2.5B this year and rising to over $7B in the next four years. Insurance companies have not yet begun to pressure companies to improve their cyber postures to get better rates, though there is some indication that it is coming. What has happened is that the role of cyber insurance has become dramatically more prominent. Almost every company has some form of insurance and it is part of basic cyber strategies in most industries. In fact, there is a case for a company not fulfilling their fiduciary responsibilities by not having enough insurance to cover a major cyber event.+
A major issue with cyber insurance, however, is that standard policies, and even definitions, have not spread throughout the industry. For that reason, every policy covers different things, in different ways. A sound business decision requires both an understanding of the technical nature of the business as well as a savvy understanding of the cyber policies. For example, most companies today just get a blanket policy that they hope covers what they need. There is little understanding of how much insurance is needed, what should be insured, what should be paid for by a claim and the threat against the company that could trigger the insurance coverage.

The Cross Over Insurance Challenge with Internet of Things (IoT)

The recent St. Jude’s medical security event discussed above presents another major challenge to businesses and the insurance industry. Cyber insurance has traditionally been focused on breaches of information such as credit card or medical records. Because Muddy Waters exposed a previously unknown vulnerability, the St. Jude’s incident brings a host of other business areas into consideration.

- What is covered under General Liability insurance, property insurance, business interruption insurance, etc.?
- If the report by Muddy Waters impacts the impending sale of St. Jude’s, which insurance policy covers such an event?
- Which policies cover each part of an incident? For example, when dealing with automobiles, what if a car gets infected by a malicious attack, causes the car to fail and creates a physical or human disaster?

As senior business leaders, the mitigation of risk is a key part of the job description. Whether from the perspective of the product developer to the utilization of technology, knowing the risks to the company is essential to the proper operation of the business. Insurance is central to the mitigation of risk, and the cross over with IoT is not something that can slowly evolve. The insurance industry, business leaders of all sectors and even the Federal Government need to address how risk will be mitigated in the IoT age.

Insurance as an Essential Element to Infrastructure Protection

Imagine the impact to the country after a major hurricane if there was no insurance to help rebuild the infrastructure damaged by natural disaster. Insurance is a critical element of the nation’s ability to respond to events, both natural and manmade, and essential to our resiliency. The discussion around cyber insurance has focused heavily on breach response and data loss incidents. As the worlds of IoT and critical infrastructure become the center of the cyber discussion, the ability of the insurance industry to respond to major cyber-attacks against these areas becomes essential to commercial and Government response.

How would costs such as large scale enterprise replacement, major economic loss, customer response, regulatory fines and litigation be covered? In talking with several business leaders, many responded “I am sure this is covered by my General Liability policy.” In talking with insurance providers the response has been “it depends on the incident”.

The Cyber Brief Is No Longer the Boring Part of a Board Meeting
A key component in this discussion is the viability of the insurance industry itself in this type of scenario. Insurance companies go to great lengths to minimize their aggregate risk in case of a large scale event. Insurers will only insure so many houses and businesses in a certain geographic area such as flood zones or hurricane areas. They insure at limited levels in different industrial sectors. All of this is good risk management practice.

These are questions that are essential to the well-being of the insurance industry and resiliency of the country:

- How does an insurer mitigate aggregate risk in the cyber domain?
- Do they only insure so many Microsoft or Google based businesses?
- Are policies limited by attack types such as hospitals and trading firms?
- In the IoT world, is there a new analytic field growing to show how many IoT devices use the same microcontroller so insurance companies can evaluate their risk?

They Didn’t Teach Me This in Business School

Imagine an entrepreneur has developed the next great IoT product that can rapidly take over the market if it can be built and deployed in the next six months. As a good business leader, the entrepreneur has developed a business plan that says if he can sell 500,000 devices at a price point of $20 per unit, he has a solid business model. Before he proceeds, however, his security lead informs him that the current design is not highly secure. A better design that includes better communication methods and different partners can be developed but it would increase the cost of the device to $30 per unit. All indications are this price increase would break the foundations of the business plan and the underlying market analysis. What does the business leader do? These decisions are not that unusual in most businesses, from automobiles to children’s toys, and are regularly made by product developers. What is different in the IoT world is the lack of data to make such decisions.

The speed of technology is moving at such a pace that the foundational data such as legal case law, insurance costs, replacement costs, etc. are not well known. The St. Jude’s case is a good example of where this lack of IoT data had significant affect. The call by Muddy Waters to sell the stock short was based on the belief that St. Jude’s would not have the financial wherewithal to fix all of the fielded pacemakers and defibrillators. Since there are no examples of a widespread attack on imbedded medical devices, how does Muddy Waters know this to be the case? If no attack occurs for ten years, is this even a concern? What is the likelihood of such an event versus the risk of replacing devices? In short, the technology speed, and associated consequences, are out pacing the availability of critical business data.

The Need for Cyber Risk Quantification

The insurance and business decision areas mentioned above both have one fundamental need that is currently not addressed well in the market: the quantification of cyber risk in terms of dollars and cents. The common language of business is money, and evaluating the size and type of an insurance policy or evaluating how much security to put into an IoT product eventually has to be translated into financial terms.
The pressing need to quantify cyber risk is where the other major event of the last several weeks becomes important. The identification of the FAIR model for quantification of risk by NIST gives a path forward in this essential business element of the cyber world. The model has a strong international support structure and its use is growing rapidly. The key element is not whether the model is perfect as much as an agreement across industry of a common, standard model. From there, new processes, tools and implementations can be developed.

Additionally, the St. Jude’s event identifies the need for companies to have a capability, either internally or outside contracted, to understand both the operations and cyber risks of the company. Once quantification of risks becomes more prevalent, then companies must be able to have a partner working with them that has deep infrastructure and operations experience that can conduct trade off analysis in both business and technical terms.

By quantifying risk, the discussions as to how much and what type of insurance also becomes more straightforward. The business decision becomes about dollars and cents, not emotional views of what bad things might happen. Most importantly, data collection can have a more focused approach that can have direct value to the consumers of the data.

If the cyber risk in the St. Jude’s medical device incident was a quantified number, the discussion would have dramatically changed. If St. Jude’s had stated that the quantified risk of the vulnerability was evaluated and planned for, then the impact of the MedSec report would have been diminished. St. Jude’s would be able to respond to investors on their calculated risk for the identified product vulnerabilities and investors could make logical, not emotional, decisions as to whether to sell or hold the stock. Abbott Laboratories could have made business decisions based on the financial risk level of the vulnerabilities in their acquisition process.

Returning to the example of the entrepreneur, with quantified cyber risk, he would have solid data to determine if increasing the price of the product is worth the increased security risk. There would be logical business data for a decision that can be presented to investors and regulators.

**A Much More Interesting Board Meeting**

The topics addressed here are just a few of the many business discussions happening in almost every major company today. The involvement of legal, public relations, finance and risk officers in the cyber discussion makes the CISO brief a key topic at any board meeting. Most importantly, moving to a quantified cyber risk discussion allows all of these groups to fully participate in and discuss the cyber threat and response in a common language.

FAIR, and the associated tools such as RiskLens, is being adopted across most of the major sectors as a method for quantifying cyber risk. As with any model, it is only as good as the available data. The growth of companies such as Advisen, Net Diligence and others to provide data is fueling the refinement of calculations. Furthermore, Government groups such as Department of Homeland Security Cyber Incident Data and Analysis Working Group are also collecting data that can be used in risk quantification. This is making the quantification of cyber risk a viable endeavor for most companies.
Now the security brief at the board meeting no longer has to be a boring list of potential vulnerabilities that nobody understands. The discussion can focus on the impact to the core business and what steps can be developed to reduce that risk. The discussion might actually be interesting enough that members don’t check their email on their cell phone.

-------

About the Author

Chip Block is Vice President of Evolver, Inc., (http://www.evolverinc.com) a major supplier of cybersecurity and infrastructure services to the commercial and public sectors. Mr. Block has worked extensively in the cyber research, development and operations field for over fifteen years and been awarded several high level honors for his advanced technological achievements. He is a frequent speaker at technology conferences on cybersecurity, cyber risk and cyber insurance. He is the architect of the Cyber Risk Ecosystem and has authored several whitepapers including “And then the Accountants Showed Up: How the Insurance Industry Will Drive Cybersecurity”. He can be reached at chip.block@evolverinc.com.