

A photograph of two women in a professional setting. One woman is seated at a wooden table, looking at a laptop. The other woman is standing and leaning over her, pointing at the screen. The scene is brightly lit, possibly from a window. The text 'HOW TO SELL CYBER SECURITY TO YOUR BOARD' is overlaid in large, bold, white letters on the right side of the image.

HOW TO SELL CYBER SECURITY TO YOUR BOARD



THE THESIS

I have argued for a long time that much of the reason that C-level executives and Board members seem confused by or out of touch with the realities of cyber-threat is because CISOs have not been very effective in communicating with those decision-makers in language they can understand.

As a CISO with 20 years of experience in cybersecurity with CISSP and CISM certifications and a co-founder of the company who created the industry's leading data center information security product, I have a little knowledge about what happens on the battlefield.

And having spent half of my career in sales, product and strategic marketing, I know a little something about the business of persuasion.

So, it occurred to me that there might be an opportunity to share what I have learned in both fields and combine that knowledge into some friendly advice about how we might better approach the dynamic between CISOs and their customers on the executive team.

That is what this little essay is trying to accomplish. I hope you all find it useful and I wish you the best of luck in advancing a cyber-defense program where your whole team can work together toward a common and urgent goal.

EMPATHY

The heart and soul of any marketing campaign is empathy.

You have to be able to take the customer's perspective and make a human connection.

It's easy to lose the human connection when you're writing or speaking about malware, detection, risk, vulnerabilities and threats.

That empathy for the people, the audience, the 'buyer', should be what drives your content, your messaging and your brand personality.

You didn't think you had a brand personality, did you? You may also believe you don't need one.

But the truth is that your CISO role already has been branded, and it might not be in a way that you would like.

If you are like most CISOs, you are likely branded as that annoying person who runs around yammering about audits and compliance, controls and process, regulations and policy, and exotic technologies while constantly complaining about being understaffed and over-worked.

If that is you, you need a new brand.



BRAND PERSONALITY

A brand personality allows you to express an opinion through stories.

Opinions are important because they convey a sense of urgency about your story. Without an opinion, there's no passion.

Opinions challenge your prospects to think. You want them thinking about the 'why' you are selling them and not the 'what'.

Instead of getting the Board to sign off on additional spend because it will do this and that to prevent future malware attacks, get them to sign off on an investment because they will be doing the 'right thing' for the organization and your shareholders while making themselves look and feel good at the same time.

You are the CISO, and thus have credentials which establish and confirm your authority. But, authority by itself is not enough.

If you want to prevail in your role as trusted advisor, you must combine that authority with a brand personality that compels cooperation from your C-level and Board members because they recognize you are on the same team as they.

And that you're not, in fact, an alien.



MARKETING

This means talking with them in terms they can relate to, and not in technical jargon that means nothing to them.

Your brand personality needs to insist through your actions, communications and demeanor that you are all about de-risking your organization and that the trail you blaze is designed to accommodate their needs, and not yours.

You will need to develop marketing skills that can persuade your prospects that what you are selling them is the absolute best thing for them.

And for your organization.

Thinking about becoming a marketeer is likely distasteful to you and worse yet, imagining yourself in a (dreaded) sales role probably borders on disgusting.

Right?

But the truth is that selling increased prevention, protection, detection and remediation are all part of the necessary process to mitigate risk in your organization's exposure to cyber-threats, which is why you are there in the first place.

Isn't it?



EMOTIONAL CONNECTION

This means that you have to weave your threat prevention, detection, mitigation and data privacy pitch into a story.

Your audience cares nothing about charts and graphs or cybersecurity statistics. They have zero interest in malware variants or exploit kits.

Stop talking about them.

Your audience cares only about impacts and risk.

You will need to create a story that provides a hook through which your audience can connect. That hook needs to be emotional. The facts are that all buyers are driven by a 'want' to buy, versus a 'need' to buy.

While much of the popular opinion believes that C-level buyers rely heavily on detailed data and rigorous analysis when evaluating a spend decision, recent research (at Harvard University) indicates that this is not actually the case.

By studying buyers' unconscious physical reactions, researchers found that what they really think or feel often contradicts what they say. This is because in fact, they are driven by unconscious urges, the biggest of which is emotion, and not intellectual analysis or the result of studying benefits or downsides.



In addition, studies by neuroscientists have found that people whose brains are damaged in the area that generates emotions are completely incapable of making decisions.

By concentrating only on the data, metrics, charts, graphs and attributes of your funding request, you will miss the unconscious and very human element in the decision-making process ... known as feelings.

Unconsciously driven by feelings, your Board and C-level buyers must be engaged and impassioned by the interaction with your story.

In other words, you need to get buyers to WANT to buy what you are selling.

Your audience is only interested in how you will make their world a better place for them to live in. And your audience only speaks finance with an emphasis on profit and loss, risk and reward.

As a result, your story needs to be relatable to an audience that is driven by either fear or gain and uses actual risk expressed in monetary terms to communicate the future state of their world if they choose X over Y.

You cannot reach that audience with data that expresses risk in terms like low, medium and high.

CYBER-RISK, NOT CYBERSECURITY

Your audience is used to making risk decisions based on financial impact to the business.

An example might be a decision to spend X to open a new retail location in a booming urban area.

That decision is supported by detailed data expressed in financial terms relating to potential upside and downside in dollars and cents depending upon A, B, and C happening and factoring the probabilities of each event occurring.


Your audience doesn't know what to do with a risk decision that begins with a thesis characterized by low, medium and high tied to probabilistic events that are based on variable historic data.

But that audience *DOES* know what to do with a story like the following that you can imagine telling to your Board for a similar vulnerability:

A CYBER-RISK STORY: EQUIFAX

Equifax was breached due to a failure to apply certain patches to known vulnerabilities in some software.

The cost of that breach to Equifax thus far is \$1.6 billion in cash and over 100 pending class action lawsuits with a potential liability award in excess of \$50 billion.



The ongoing legal expense to support this litigation is in excess of \$18 million per month. The cost to apply those patches was less than \$200K.

We have the exact same vulnerability on the software we use to run our web services. We have similar information assets at risk.

The direct cost associated with the loss of our customer data for recovery and replacement alone is \$100 million (analytics attached).

RISK CALCULUS

The ancillary costs associated with increased credit cost, reputational damage, increased insurance premiums, contract forensic services and legal expense is \$137 million (chart attached).

The probability of our company being attacked through that vulnerability in the next 12 months is 80%.

This is because 18 companies just like ours with similar vulnerabilities have been attacked 7 times in the last 12 months (chart attached).

The potential impact is reduced to 5% if we apply the patches (as Equifax learned the hard way).

To act, we will need \$200K as an investment to hire resources to perform the work.

The risk calculations follow.

RISK = PROBABILITY x POTENTIAL IMPACT

The risk if we do not act is \$189.6 million (risk = probability x potential impact).

The risk if we act now (increase our cybersecurity investment by \$200K) is \$4.7 million.

PERMISSION TO DECIDE

This story uses terms that your Board and C-level buyers can understand and relate to.

In addition, the story strikes at two important emotional drivers. Fear and safety. And you provide hard data to back it all up. Data is important, but buyers don't make decisions based on data. They only need data to give themselves permission to decide.

Whether it's an investment to address new threats from cloud computing or endpoint protection or IoT or BYOD/C, or whatever, there are countless stories throughout our recent history that you can incorporate into your pitch.

They are relatable because they are in the same sector or because similarly placed executives lost their jobs or because they acted wisely and avoided a missile strike just like your wise board will surely do.

After they hear your story.



CONTEXT IS KING

While you are thinking about your story, keep in mind your audience context.

Delivering a technical view of cyber-risk will completely confuse your business-centric Board.

Instead, you need to provide them with useful information so they can compare your investment against the other set of enterprise risks in competition.

ALWAYS A BUSINESS PERSPECTIVE

Start your communication by introducing risks from a business perspective, i.e. “We have 22 internet-facing hosts, and 12 of those sit on infrastructure owned by an external entity. We have never conducted a third-party risk assessment. The assets sitting on those hosts are worth \$100 million. We have very similar vulnerabilities to those that caused the Target breach. It is critical that we conduct a third-party risk assessment immediately.”

This gives your Board enough information in their own language so they can understand the fiduciary threat.

And, because the Board communicates and operates at a strategic level, tailoring your conversations appropriately and using a business context to prioritize a handful of business critical risks will cement your position as a member of their team.



LEAD AND TEACH

As the CISO, your job is to guide the Board to recognize and acknowledge the realities of today's threat landscape.

You need to help them understand that every expansion joint in the business model invites increased risk into the equation.

If the Board wants to open up your environment to 3rd party vendors, the entire organization's risk will increase. Ditto, if they offshore manufacturing. If they decide to move to the cloud or adopt BYOC policies, your risk will explode.

Teaching your Board about these threats and the associated risks provides them with useful insight to better govern the organization and further burnishes your credential as a proactive and helpful member of the team.

FREQUENT AND CONSISTENT

In the case of TPA's for example you might suggest establishing a process for regular assessments. A series of rigorous red team testing and controls audits conducted quarterly will give your Board some necessary confidence that progress is being made.

Just make sure you communicate in fiscalez.





CEO GUIDANCE

Another one of your jobs is to help the CEO manage the business. This requires that you are able to tie cyber-risk to business operations.

Giving the CEO cyber-intelligence that they can weigh against other initiatives will improve their ability to balance between conflicting priorities.

But, that intel needs to be in the form of financially quantified data. Low, medium and high means nothing to your CEO. Or, anyone else for that matter.

CAPTURE QUANTIFIED RISK

There are new solutions on the market that feature multiple integrations and a high degree of automation.

Some provide the identity of quantified asset values at risk throughout your network in near real-time. They can identify threats and vulnerabilities tied to specific asset values hosted or processed through various network devices and fire alerts when critical data is under siege.

Collecting relevant risk information and presenting actionable options to manage that risk in financial terms, will enable you and your CEO to make rational, proactive decisions about acceptance, transfer or mitigation.

This will make you look like Captain America.

YOUR CFO

CFOs are used to evaluating technology investments in the form of “programs.” Programs usually include components like spending projections, ROI, and “technical debt” that is incurred based on postponed or delayed investments.

“Technical debt” is a potential cost to the business of deferring investment in a particular technology at a given point in time.

Your CFO is going to expect a similar proposal for your cybersecurity investment recommendations.

You will need to be able to demonstrate how proactive investment in cyber-resources stay aligned with business initiatives and put your organization out front and ahead of developing risks.

HERE IT IS CRITICAL THAT YOU SPEAK QUANTITATIVELY AND IN DOLLARS.

Old school quantitative scores for risk assessments like a 498 are meaningless. But, if you identify a risk that is quantified at \$498 million with a 20% probability of loss, your CFO will be able to compare that data with similar data for other enterprise risks and investments on her desk.

Remember, you’re Captain America now.





A FRAMEWORK

Most CISOs are comfortable with frameworks. Which is good because we are suggesting one that will work effectively for your Board communications.

If your presentations are framed within a model of cyber-risk that is familiar to your Board, you will have a much better chance of being heard.

FOUR ATTRIBUTES OF CYBER-RISK

This model structures four attributes of cyber-risk with an attacker at its core.

- 1. Probability. What is the Probability the risk will occur?**
- 2. Susceptibility. What is your Susceptibility to that risk?**
- 3. Severity. What is the Severity of that risk?**
- 4. Urgency. What is the Urgency of that risk?**

The importance of the attacker is motivation. Understanding motivation helps determine the relative impact of all four attributes.

No more chatter about CVSS 3.1's, malware strains, attack vectors, patches, technology features, vulnerability reports by device and asset, exploit code maturity levels, ya-da-ya-da-ya-da-ya-da.

Just probability, susceptibility, severity and urgency along with attacker motivation. This makes sense to normal people. Like your Board.



BUSINESS OBJECTIVES

Technology may be where a cyber-threat begins and how it will be mitigated, but the business impact is why it matters.

The key to reaching your audience is to de-emphasize the technology and double down on the business impact.

That's why you need to frame your story in language that the business understands.

Some smart folks at Harvard suggest each story be framed within these four business objectives:

- 1. Availability: Keeping business processes running, and recovering from failures within acceptable timeframes**
- 2. Access: Providing information to the right people while keeping it away from the wrong people**
- 3. Accuracy: Ensuring information is correct, timely, and complete**
- 4. Agility: Changing business processes with acceptable cost and speed**

The value of each objective depends on the stakeholders impacted.



IMPACT VARIES BY STAKEHOLDER

For example, you and the IT team will prioritize availability and access. Your Chief Revenue Officer will be most concerned with access and accuracy. Your buddy, the CEO focuses on all four objectives.

As you address each audience, you should tailor your story to integrate their business objectives so that you can maintain the business context.

This will enable your audience to participate with you in the prioritization of cybersecurity and risk initiatives as they will be viewing the challenge through their own lens.

Not yours.

INVESTMENT, NOT BUDGET

The narrative in your stories needs to focus attention on the investment required to achieve value in return.

Telling your story in cyber-risk calculus will enable your audience to begin recognizing your function as a business enabler and not just a cost center.

Your ability to view the business through the prism of risk management will engender confidence that you can help make the business run faster, reduce losses, and more intelligently manage cybersecurity expenses.

Aka real ROI.



YOUR NEW BRAND

Perception is reality.

Moving away from your perception as the annoying cost center sink-hole who is constantly getting in the way of LOB progress is actually easier than it sounds.

It starts with your ability to begin framing cybersecurity challenges in a cyber-risk context in line with business objectives.

CRITICAL RISKS IN BUSINESS IMPACT TERMS

Regular and frequent communication with the Board and your C-suite where you consistently identify the 2-3 most critical cyber-risks in business impact terms will quickly move you toward 'trusted business advisor' status.

DEFINING RISK APPETITE

When you are able to measurably impact the business through helping your organization define its risk appetite and by identifying alternate paths to mitigate risk, in language and models that are understandable to your Board and the entire C-suite, you will finally be seen as a certified and participating peer member of the executive tribe.

And, yes ... it's about time.