Let's Talk about Security Health…

Carlota Sage, Founder of Pocket CISO

Until I got into information security, my greatest gift to the world was getting Netflix to stop calling its Spanish members “miembros.”

In 2012, I was on a (pre-video) conference call with our Latinx call centers and announced the roll out of the much-requested Spanish translations of the Netflix Help Center, only to be met by stone cold silence. After what felt like an eternity, a voice very quietly asked, “*We don’t call our subscribers ‘miembros,’ do we?*”

“*Well, yes, that’s what we call them in the interface…is it a problem?*” More silence. I was getting an uneasy feeling about this. Finally: “*Uh…we don’t say that word on the phone.*”

Confused, I asked why, but the director suggested he’d fill me later. It turns out, just as in English, the word *miembro* could denote ‘a person within a group,’ or it could be used to mean a particular appendage. And according to this director, the further south you went, the further south the meaning went, as well.

I emailed this concern to Marketing, letting them know I was changing the word in the Help Center and they needed to change it in the interface, as well. A gentleman in LA whose parents came from Mexico City insisted this was not the case and I should not change anything. I responded that I had 110 people on the ground who would not use this word on the phone for fear of offending someone’s *abuela*, so it would not be used in the Help Center. I changed the word; I’d rather get fired for doing the right thing than keep working knowing I’ve chosen to do wrong.

A few months later, after a focus group or two, Marketing sent me a note giving me “permission” to make the change that I’d made at the very beginning.

What does this story have to do with InfoSec?

Even when we’re experts at a discipline like Marketing or Security, it doesn’t make us the expert in our customers’ needs. NIST, CMMC, and other maturity models were made for security practitioners - and not for the executives, business leaders or employees they serve. Even when we’re speaking the same language, we’re not speaking *their* language.

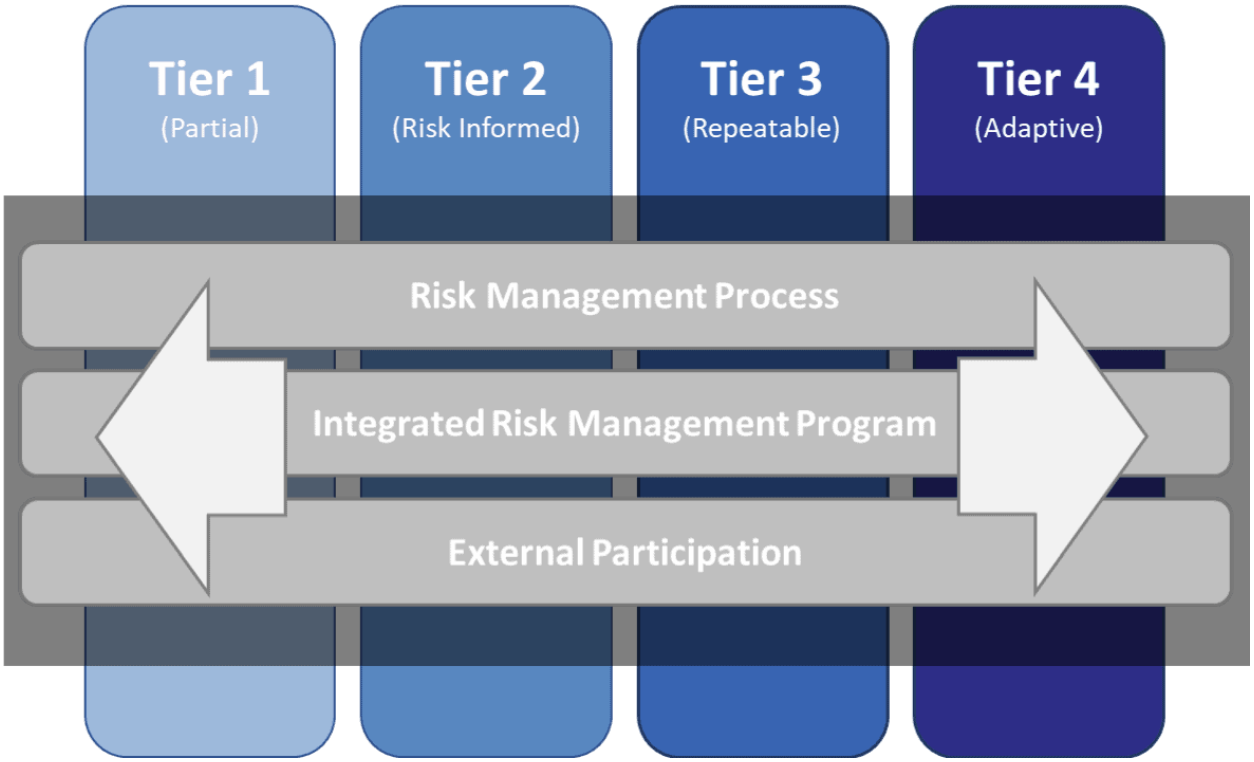
More importantly, just as Netflix needed to stop calling their Latinx subscribers *miembros*, we need to stop saying “security maturity” to our business leaders. “Maturity” has a connotation that

you continuously get better or more sophisticated, and that's simply not the case with cybersecurity. It's much easier to lose traction with your security program than to grow it - we need to talk about healthy and unhealthy security habits with our business peers. Stop talking about *Security Maturity* and start talking about *Security Health*.

So what's wrong with the NIST Maturity Model?

Simply put, it's jargon. What's worse is that we throw the NIST Maturity Model at folks while we're talking jargon at them. Don't get me wrong, the NIST Maturity Model is great, *if you're a security person*. But for a non-security professional, the model assumes you know enough about security to interpret it. For one, It assumes the viewer understands the relationship between information security and risk management. The arrows denote some kind of movement between tiers, but assumes the security professional knows what contributes to that movement. Can anyone who isn't experienced, hasn't read a book or hasn't spent a few hours pouring over NIST documentation convey what's in this model?

Figure 1: NIST Security Maturity Model



If you look at the CMMC and NIST Risk Management Hierarchy, they suffer the same weakness - you need to have a reasonable knowledge of security for these models to be useful. Even with

documentation, these models are about the security practitioner's implementation of security processes rather than communicating security to the business. These models are very much needed – but not very helpful for a CISO, vCISO, or someone trying to start a security program to bridge the communication gap with organizational leadership.

I searched the Internet for other maturity models and found some decent ones by consulting groups, but, frankly, I often found the language they used insulting or fueling "FUD" (fear, uncertainty, doubt). These are rampant problems within our industry: security experts talking down to anyone who isn't a fellow security expert, or using fear to sell security products and services. I realized I could solve two problems with one model – I could make a model meaningful to business professionals while giving a great example of how to talk about security without using a condescending tone or resorting to FUD.

What key concepts did I need to communicate to my client about cybersecurity?

There were several things I feel are important to communicate to an executive team and board to ensure not just initial, but ongoing support for a security program.

1. *Security has an organizing principle.*

   Even if your organization doesn't have a security or compliance team, someone or even a whole team is probably practicing good security hygiene in their little corner, or some teams have implemented security basics in response to regulatory and compliance requirements. But the best way to approach security is as an entire organization, and that requires, well, organization!

2. *Your organization's awareness of security impacts your security health.*

   Your organization's security depth is directly proportional to the number of people in your organization who understand security basics and practice them. This requires you to have a shared understanding of security throughout your organization – from your employees to your executive team to your board of directors.

3. *Your organization's culture impacts your security health.*

   If your organization is highly siloed or communication across teams is poor, your path to security healthiness will be more difficult. A security program may highlight cultural weaknesses.

4. *How you use technology is more important than what you use.*

   You could spend all the money in the world on technology and tooling, but you'll never achieve security *healthiness* if you're not using that technology in a way that best supports your organization's business objectives.

5. *Security requires leadership to stay healthy.*

   The executive team has to be one hundred percent committed to securing your organization for it to be successful. More importantly, they need to have meaningful insights and metrics that help them best understand how security is reducing the organization's overall business risk, and to understand when they need to invest more into or change how they're investing in the security program.

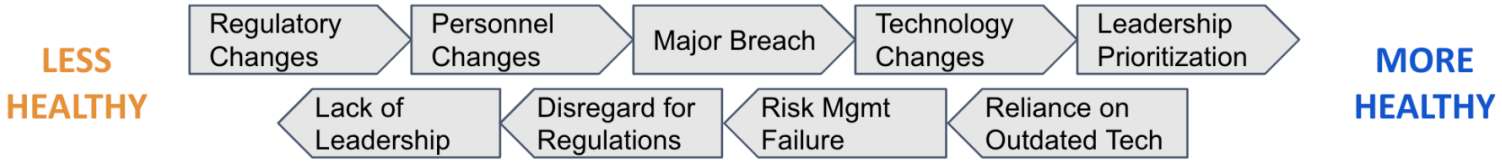
6. *Security requires constant vigilance to stay healthy.*

   Security isn't a "climb to the top of the mountain" activity, where you're done once you've reached the peak! No, security is a "steer the ship through the rocks to keep the boat from running aground" activity. There is almost never a "set it once and done" task or technology in security.

With these things in mind, I drafted the first security ~~maturity~~ health model in early 2020. It lives in a GitHub repo under Creative Commons so anyone could use it.

Figure 2: Security Health Model

	Grassroots	Team or Compliance-Driven	Risk-Based
Organizing Principle	Individuals or individual teams may take responsibility for security in their areas	Gov't regulations or customer expectations drive security measures	Security is an organization-wide risk management tool.
Organizational Awareness	No common understanding of or baseline for security across org, leadership & board	Only the team responsible for security or compliance have a definition of security initiatives	Security integrated into program and product initiatives
Culture	Security seen as a "technical problem"	Security seen as "compliance problem"	Security seen as core to enabling the business
Technology	Security exists as configuration of networking, laptop, software tools	Security tools brought in as a response to outside pressures & may not be aligned with the business	Security tooling in place to support business alignment and risk management
Ownership/ Leadership	No central cybersecurity ownership or leader	Security leadership exists in a silo focused on compliance	Security leadership enabled by and has direct access to C-Suite, Board



It's not a "simple" model, but it is a meaningful one. It manages to hit all six of the critical facets I wanted to in a single table. I was able to include enough verbiage to make each state meaningful to someone with zero understanding of cybersecurity – and without anyone having to read a book on it (unless they really want to!).

In addition to hitting the six key talking points, I felt the model embodied security health concepts in an eye-catching way that helps a business person rapidly move through it.

Driving Factors

Despite the reliance on verbiage of the organizational security health model, there are some key concepts that help move executive teams through the model.

Grassroots or Ad Hoc
In the "Ad Hoc" concept, any approach to security is on an individual or team basis and/or security is generally viewed as a problem that can be solved with technology alone. There is no organization-wide approach to or understanding of security, and no centralized ownership of the security strategy.

Team- or Compliance-Driven
In the Compliance-Driven concept, government regulations, industry standards or customer expectations drive an organization towards security. Security awareness and collaboration coalesces around compliances needs, shifting security to being a "compliance problem." Technology emphasis shifts to compliance controls, potentially endangering any focus on business risk.

Risk-Informed or Risk-Based
In the Risk Management-Driven concept, security becomes a vehicle for managing business risk across the organization. There is a shared understanding of security both across the organization and at the leadership/Board level. Security is viewed as an integral part of any business endeavor, with technology implemented in alignment with business objectives. Security strategy is centralized and has a direct communication line with the Board of Directors.

Most importantly, the model talks about “Security Health” rather than Maturity…

> *Less Healthy vs More Healthy*
>
> I found it was difficult to paint a quick picture or make a quick analogy using the “less mature vs more mature” or “immature vs mature” verbiage. Instead, I chose “less healthy vs more healthy;” in discussions, it’s easier to compare the maturity scale to grabbing a candy bar, a granola bar, or a chicken salad for lunch. No matter which one you get, you’re fulfilling the core objective of getting calories into your system. It paints a very quick image that making less healthy security choices, like only ever eating candy bars, leads to increasingly less positive outcomes over time.

Use the Security Health Model as a guide for meaningful discussions with your executive team and Board of Directors. Start with the embodied concepts to paint the bigger picture, then fill in details with the six key talking points to help leadership understand where the organization as a whole is now, and where they need it to be. Use the simplified version to keep maturity concepts fresh as you give the executive team and Board updates.

Turning the Security Health Model in to Health Checkup

Security is a classic case of the chicken and the egg:

> *How do I justify the cost of security tooling when I don’t have a security program?*
> *How do I measure my security program if I don’t have security tooling?*

I felt like the Security Health Model could help solve this conundrum, but I didn’t want to just slap a scale on it. However, after looking at other business and security models from common frameworks and consulting groups, slapping a scale on it was the most obvious evolution. If your scale is meaningful, it’s operational. By having a scale, you can better communicate where you are and where you need to be, then use it to drive improvements in security operations, even if they create a net spend.

Since there were three major themes in the Security Health Model, the simplest thing to do was start with a three point scale. I distilled the Health Model to its three key stages.

With these three stages highlighted, the scale starts to take shape:

1. Little or no consideration of information security.

2. Information security has an organization-wide structure, documentation and project management.
3. Security is considered a critical business and sales tool. Practices are repeatable, scalable and optimizable.

You can absolutely use the simple three point scale, but a five point scale gives more nuance by defining the “between” states, allowing an organization to better see its progression. The difference between a 1 and a 2, or between a 2 and a 3, on a three point scale is a big leap for a smaller organization. The difference between a 1 and a 3, or a 3 and a 5, on a five point scale better delineates a path by defining the middle ground between them.

1. Little or no consideration of information security.

2. Information security efforts lack structure and organization. Even if processes are well defined, they are generally poorly documented. Successful efforts are localized and unlikely to be repeatable or scalable.

3. Information security has basic structure, documentation and project management; there is organization-wide oversight/insight even if scalability is an issue. Security likely be driven by compliance/regulation rather than an understanding of risk management.

4. Processes are well-defined, well-documented, repeatable and scalable, incorporating data analytics for insights. Information security is a risk management tool rather than a compliance tool.

5. Information Security program or team has the experience and technology needed to provide near real-time insights to the executive team and business units. Focus is on process optimization for the entire organization, not just security.

Now that the scale was set, I had to figure out how to use it.

What are we measuring?

In Technical Support Operations, I coached a lot of support engineers on how to troubleshoot and helped technical writers with creating troubleshooting guides. In troubleshooting a problem, whether it’s hardware or software, it’s helpful to break the system down into components. Problems can happen within a component, where two or more components interact, or at the interface to the user.

That's why it's helpful to think of an organization as a system, with security as one component. We need to understand what can go wrong with the pieces internal to security (i.e., the security component), the interactions of the security component with other business components, and how security is presented or interacts with the company's customers.

With this structure in mind, the health model measures the organization as a system, including its cross-functional relationships, cybersecurity operations, and external relationships.

Figure 3: Measuring Security in an Organization

Cross-functional Relationships	
Business Alignment	*What Security needs to know about the Business*
Awareness & Training	*What the Business needs to know about Security*
Compliance & Audit	*What Business and Security need to know about Regulations*
Program Management	*How Security functions within the overal organization*
Cybersecurity Operations	
Identity & Asset Management	*Who and what security needs to secure*
Vendor Management	*What xternal services impact organizational security*
Detection	*How Security monitors assets and environments*
Emerging Threats & Vulnerability Mgmt	*What Security needs to know about external risk*
Incident Response	*How Security responds to immediate threats*
Communication Strategy	*How Security communicates what's happening*
External Relationships	
Partner Relationships	*How Security interacts with (non-vendor) Partners*
Customer Relationships	*How Security interacts with external Customers*

Public Relations & Crisis Communications	*How Security presents itself to the public at large*

Where are we measuring?

For larger or mature organizations, it's often easiest to align these metrics to existing business units: Finance, IT, Marketing, Sales, Customer Service, etc. For smaller organizations or organizations without a traditionally defined structure, it can be as simple as Internal Operations and Product Lines.

An example of an initial Security Health Check is excerpted below. This example company is measuring the security of its internal operations, along with two different products.

Figure 4: Example of Security Health Scale

	Internal IT	Product 1	Product 2
Cross-functional Relationships			
Business Alignment	2	2	2
Awareness & Training	1	1	1
Compliance & Audit	2	2	1
Program Management	1	1	1

How are we measuring?

I like to start these as team discussions; this will often bring a balance between those who gloss over things and those that focus on the negative. Later, they're easily updated as a part of your internal review or audit.

Use these questions to help you guide these discussions.

Figure 5: Questions to Consider when Assessing Security Health

Cross-functional Relationships	
Business Alignment	Do employees know what to do or who to contact if they have security questions or concerns? Do employees understand the data they handle and their responsibility for handling it securely?
Awareness & Training	Have employees completed the organization's baseline security training this year? Has leadership worked with the security team to identify additional training needs for their group?
Compliance & Audit	Is leadership aware of industry or government regulations that impact both the company as a whole and their group in particular? Is the group prepared for an audit tomorrow, and if not, how long do they feel it would take to prepare?
Program Management	Does the group include security as a consideration/ communication need in project and change management procedures?
Cybersecurity Operations	
Identity and Access Management	Is there a documented and consistently repeatable process for creating and retiring identities? Is access to critical systems reviewed at least monthly? To all systems at least yearly?
Asset and Vendor Management	Are physical and digital assets for this group included and updated regularly in asset inventory? Is security reviewed as a part of vendor or third party review and engagement?
Detection	Are the assets and systems most used by this group included in any detection platform used by the security/technical team?
Threat & Vulnerability Management	Is this group's attack surface larger than or a significant portion of the organization's attack surface; if so, is there increased visibility

	into those areas? Is this group's resources appropriately prioritized for systems patching and vulnerability management.
Incident Response	Is this group's needs included in the corporate incident response plan?
Communication Strategy	Is this group included in security communication policies/plans or any security RACI matrices?
External Relationships	
Partner Relationships	Does the security or leadership team have contact information for those responsible for security and privacy at partner organizations? Does the security or leadership team have regular (quarterly or yearly) reviews of partner security practices?
Customer Relationships	Is there an escalation path from front-line customer support and social media personnel to security? Is the security and privacy information on the corporate or product website easy for customers to access and understand? [B:B] Does the security or leadership team have regular (quarterly or yearly) communication and reviews with customers?
Public Relations & Crisis Communications	Is there an easy way for good samaritans to report issues found with your website or product? Does your organization have or participate in a bug bounty program? Are crisis communications and plans well documented and easily found by employees?

The Health Model in action…

Now let's assess one of these questions for the health model using our five point scale from above.

"Do employees know what to do or who to contact if they have security questions or concerns?" If the answer is…

- "How do I know if my question is related to security?" = 1
- "Yes, I pop into Slack and ping IT," = 2
  Follow up question = "What does IT do next?"
    - If IT has a process for handling this, great! They're still at least a 2.
    - If IT has an accurately documented process, even better! They're now a 3.
    - If IT has an accurately documented process AND that process can still function if your company suddenly doubled, this is best!! This is a 4!

It's important to note that a "3" is the baseline where processes are documented and repeatable – I tell new clients (who are usually all 1s or 1s & 2s when they come to us) that 3 is where I want them to be after six months.

Also, you'll often find that someone, perhaps even an entire team, is behaving in a security conscious way. But if that process isn't documented, that team is not achieving even the baseline of 3. All they have to do to reach the baseline is write down the existing process. That's it! So while time consuming, it can be very easy for that team to reach a baseline of 3.

IMPORTANT:

I don't expect any sub-500 person company to be a 4 or 5 – this requires a significant investment in security tooling that non-enterprise organizations usually can't afford. The goal for a smaller organization is to get to a baseline of 3 and keep from sliding backwards.

How often are we measuring?

My team at Pocket CISO creates an initial security health model as a part of the gap analysis with a new customer, then again after six to eight months together so they can see their improvement. After that, yearly for very mature/stable organizations or more often for rapidly changing organizations. The Security Health Model will help ensure that healthy security practices are maintained as an organization grows.

What does improvement look like?

Below, you'll see that the organization we looked at in Figure 4 above has made some improvements after six months of work!

Figure 6: Example of Security Health Scale

	Internal IT	Product 1	Product 2
Cross-functional Relationships			
Business Alignment	3	3	2
Awareness & Training	3	3	3
Compliance & Audit	3	3	2
Program Management	3	2	2

Getting started with Security Health!

You can download Excel files with these models, along with other handy tools under the Creative Commons license, from my GitHub:
https://github.com/carlota/showmethemoney

Please customize them to your needs and use them to better improve your organization's understanding of security health!