Cyber Security Culture Barometer

WELCOME

Introduction

This simple self-assessment is provided free of charge in an effort to help you see the impact that your organization's corporate cyber security culture has on your efforts to address cyber threats and exposures.

It consists of a simple matrix of 10 different aspects of cyber security culture each having six different descriptions of how an organization addresses that aspect. The descriptors range from outright hostility to cyber security, to totally embracing it. Your choices will determine just how supportive your organization's cyber security culture is to your efforts. The simple scoring table provides a summary assessment. What is important is not to get the 'right' answer but to pick the one that best describes your organization. Only in that way can you get value from this assessment.

If you find it of interest and would like to pursue the implications further, send an email to info@naganresearchgroup.com with the subject Cyber Security Culture Barometer.

Background

Today the pace of change in malicious cyber events is accelerating. In the past the risks were mainly in someone gaining access to valuable information such as proprietary company information, financial records, and customer credit card data, and then using the information for gain. We now see a rise in harming the ability of an organization, or an individual, to function by disabling key operations, and sometimes demanding a ransom payment to return it to normal. Additionally there is a rise in malicious exposures to harm a company's repute.

New cyber threat arise constantly, which leads to too much energy wasted on how to react to it. This is a strategic mistake. Focusing solely on cyber threats is a losing proposition as there will always be a new cyber threats. It is technologies version of cyber 'wack-a-mole'. You need to stop playing cyber wack-a-mole and begin to take the offensive against the predators that infest the cyber eco-system we all inhabit.

You need to identify and manage your cyber exposures so you are not always playing catch up. That is not to say you should ignore cyber threats. You need to deal with those that are in your cyber eco-system. Rather, if you want to get ahead of cyber threats you need to identify and deal with your organization's cyber exposures. By 'cyber exposures' we mean the vulnerabilities that arise from inhabiting the cyber eco-system. Realize that these vulnerabilities are not just technical but rooted in human behavior, legal and compliance matters, use of social media, the cloud and the Internet of Things (IoT).

A key to successfully addressing the many cyber exposures your organization faces is understanding the mindset of the members of your organization – the cyber security culture. This can be done by examining attitudes towards cyber exposure, responsibilities towards cyber security, and awareness of the cyber threats in general. In other words how does your organization view cyber security? Is it only a technical concern? Not a real problem? An annoyance to be circumvented? The answers to these and similar questions will go a long way towards understanding the approach you take to improve your organizations cyber defenses. If your culture treats cyber security poorly then your organization is much more likely to experience a cyber event.

In summary: cyber security culture matters and cyber security culture can be managed.

Cyber Security Culture Barometer

Welcome to the Cyber Security Culture Barometer. The first step to determine if your organization's cyber security culture will support your efforts in securing your cyber environment.

On the next page you will be asked to choose descriptors that best fit your organization. Then choose the number of the descriptor and enter in the appropriate box below, sum up the score and use the table to get a quick reading on how supportive of your efforts your organizations cyber security culture will be.

We hope you find this of value.

If you would like to learn more follow the instructions below.

Be Secure and Be Safe.

Rating	Aspect
	Attention paid to cur cyber security culture as well as the technical issues
	Cyber exposure prevention over reaction
	Approach to cyber security
	Assessing cyber exposure and our culture
	Relationship building
	Education regarding cyber exposures
	Cyber security standards and audits
	The "Why", the "Who?" and the "How?" of cyber security
	Cross organization organization and cooperation
	Vigilance regarding cyber attacks
	Total of the above Aspect ratings

Quick Scoring Summary

Add the numbers above, place the total in the last box then look up the range they fall in to get a quick assessment of the support you can expect from your cyber security culture.

0-20 A very toxic cyber security culture with significance issues that need immediate attention.

21-40 A toxic cyber security culture that has issues that need attention.

41-60 A cyber security culture that needs significant work to be fully supportive.

61-80 A healthy cyber security culture that needs to be improved but is on the right path.

81-100 A very healthy cyber security culture that needs to be nurtured and maintained.

Additional Services:

We hope you have gained some insight into the factors relevant to a supportive cyber security culture. If you would like a more detailed analysis regarding your selections, as well as a copy of our book, 'effective Cyber Exposure Management', you can do so by sending an email to info@naganresearchgroup.com and have the subject 'Cyber Security Culture Barometer. The book and detailed analysis cost $59. Instructions will be sent upon receipt of your email.

Cyber Security Culture Barometer™

The "Climate" necessary to minimize cyber losses.

Your Culture

What are we trying to measure and why is it important?

We have picked 10 aspects, along with 6 descriptors for each, that are instrumental in defining an organizations cyber security culture.

We believe, and our research supports, that an organizations culture can make or break a project, including cyber security. If your culture is 'toxic' to cyber security then success is not likely.

There are no 'right' answers what is important is to choose the descriptor that reflects, as near as possible, your organization.

You can then use the first sheet and choose the number of the descriptor selected.

There is quick scoring summary so you can see if your cyber security culture is supportive or toxic. For a more detailed analysis complete the instructions on the first page and email your choices for a analysis.

Good Luck!

	Descriptor / Aspects		Aspect Ignored	Aspect is Controversial	Aspect is Valued	Aspect is Accepted	Aspect is embraced	Aspect fully supported
			0	2	4	6	8	10
	1	***Attention paid to our cyber security culture as well as the technical issues***	We don't pay any attention to our cyber security culture since we don't think it is important in relation to our technical expertise.	We occasionally mention our cyber culture but rarely do anything about it.	There is some awareness of the importance of our cyber security culture but not much has been done to define and measure it.	We know that cyber culture is important and have taken some important steps to define and measure it.	Our awareness of the importance of our cyber culture is growing. We will soon have the systems we need to balance our social and technical approaches.	We pay equal attention to both our cyber security culture and our technical issues. They are always in balance.
	2	***Cyber exposure prevention over reaction***	We have no prevention strategies or programs relating to culture or social aspects of cyber security. We react to cyber intrusions as they arise. .	We are starting to respect the concept of prevention over reaction but it is not usually readily evident.	We think it is right to favor prevention over reaction and have started to move in that direction.	We believe in prevention over reaction but still have a way to go.	We are working hard to avoid the need to react by doing more prevention and we are pretty successful.	We are meticulous about making sure that we advocate prevention over reaction. Every time we discuss cyber security we focus on prevention.
	3	***Approach to cyber security***	We have embraced a narrow view of cyber security that focuses on specific "technical issues" and ignore the rest.	We are not sure about what we should be doing but we are thinking about broadening our approach to cyber security.	We recognize that our approach to cyber security is shortsighted and have begun to expand our efforts.	We've started to address the flaws in our approach to cyber security and have made some noteworthy progress.	Our approach to cyber security is greatly expanded and enhanced and we are nearing a "state of the art" approach.	We have a comprehensive approach to cyber security that includes every known aspect and is always looking for new exposures from everyone.
	4	***Assessing cyber exposure and our culture***	We do not have any kind of ongoing assessment of our cyber exposures or our cyber culture.	We realize that there is virtue in assessing our cyber exposures and the culture necessary to avoid losses but have barely started to act on the knowledge.	We know it is right to have a consistent approach to cyber security and to constantly assess both the exposure and the culture but we have much to do.	We are becoming proactive in developing programs and processes but still have a lot to do.	We recognize that we can still do more but we continue to make progress and can "see the light at the end of the tunnel."	Our assessments of our cyber exposures and our cyber culture is ongoing and everyone "buys in" to the need for those efforts.
	5	***Relationship building***	We have little or no collaboration with fellow professionals, business partners and their organizations when it comes to cyber security.	We are starting to see that relationships have the potential to help us with cyber security.	Commitment to widen our relationships to enhance our cyber security is growing.	We are deploying more resources to improve our relationships and they are growing and our cyber security is benefitting.	We still have some unfinished business when it comes to relationships that are enhancing our cyber security but we are close.	The desirability of learning from and with those who have common interests with us is fully accepted and acted on at every opportunity .
	6	***Education regarding cyber exposures***	We feel that education is overrated. So the concern with cyber security is the dominion of very few of us and others are rarely enlightened.	We recognize the need to enhance our cyber security education but we've just gotten started.	Confidence is growing that education is part of the answer to our cyber security and we've made some noteworthy progress.	We all know that education is a primary ingredient in our cyber security and we're acting on it and have made progress.	We are refining our approach to cyber security education for everyone and are approaching our goal of optimizing our efforts.	We always respect the potential benefit of cyber security education and the participation of every associate in our cyber security efforts.
	7	***Cyber security standards and audits***	We have no cyber standards and hence have no audits since we have nothing to audit against.	We recognize that we need cyber standards and we need to audit against them; but we are just starting to act on that knowledge.	We fully understand the need for cyber security standards and audits and have begun to develop them.	We not only understand but are well along in creating and implementing cyber security standards and an audit program.	We have developed and implemented a set of cyber security standards and now need to audit and refine them based on experience.	Our cyber security standards are clear and easily understood and we have regular audits to insure universal understanding and practice.
	8	***The "Why", the "Who?" and the "How?" of cyber security***	We fail to understand and act on the foundations for cyber security. So our ability to answer and act on the "Who?" and the "How?" is seriously deficient.	We're realizing that the most important factor in good cyber security is why we do it within our values. We have begun to act on that knowledge.	We're starting to regularly consider why we need exceptional cyber security and act on those considerations.	We respond to motive as much or more than to who does what and how they do it since we know the "why?" is the foundation.	We are getting very good at knowing our cyber security values and acting on them.	We not only believe in the importance of the moral imperatives of good cyber security but every action we take is based on that knowledge.
	9	***Cross organizational cooperation and communication***	We are insular and are very reluctant to reach across organizational boundaries in our cyber security efforts.	We recognize that we have to reach out all the time and build bridges across the organization.	We not only recognize the need to build bridges but are acting on the knowledge more every day .	We are beginning to internalize the need to always reach across our oganization with common values and collaborate with others.	We are close to our goal of total inclusion so mutual benefits with those of common interests are the rule.	We never miss an opportunity to learn from others by cultivating friendships with anyone who may have common interests
	10	***Vigilance regarding cyber attacks***	We are often oblivious to cyber incursions and so have a history of "too little too late" when it comes to reacting to attacks.	We are beginning to realize that without constant vigilance we are always vulnerable.	We recognize the centrality of constant vigilance when it comes to our cyber security, and we are beginning to act on that knowledge daily.	We are deepening our grasp of the importance of constant vigilance and well past the midpoint of where we want to "go."	We encourage everyone to be constantly vigilant and the "message" is getting through almost all the time.	We are fully committed to vigilance so we are sensitive to even the threat of cyber loss and react promptly to even the suggestion of an incursion.

Comments: