How Corporate Culture Impacts Cyber Security

By John R Childress
Chairman, PYXIS Culture Technologies

How Corporate Culture Impacts Cyber Security

"Threat is a mirror of security gaps. Cyber-threat is mainly a reflection of our weaknesses. An accurate vision of digital and behavioral gaps is crucial for a consistent cyber-resilience." ~ Stephane Nappo

In 2020, the global spend on cyber security was around $150 billion, and is expected to grow at 12-15% through 2025 [1]. With that amount of focus and money spent on cyber security protection, it would seem reasonable to assume that we are well protected from cybercrime.

Wrong!

In the first 6 months of 2021, companies paid out $1 trillion in ransomware extortion alone [2] and by 2025 the global cost of ransomware is expected to be $10.5 trillion [3]. It's not just large companies or global financial institutions that are impacted by cybercrime. Forty-three percent of cyberattacks are aimed at small businesses [4], most of whom have rudimentary cyber protection at best. To make things even worse, there is a growing trend of cyberattacks on hospitals and the healthcare industry, where a loss of access to network systems and data could result in loss of life.

$ 1 T	485%	43%	90%
Ransomware payments first 6 months of 2021	Increase in global ransomware attacks between 2019-2020	Of cyberattacks are against SMEs	Breaches from human mistakes and errors

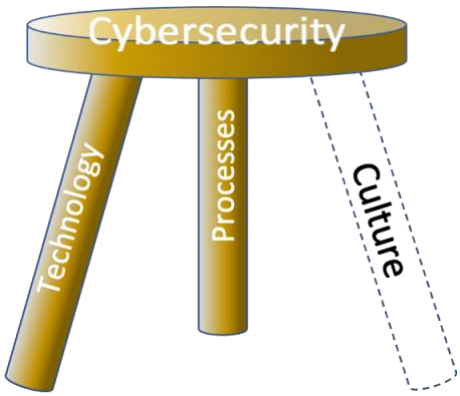
Okay, so more technology is not the solution to effective cyber protection. In fact, the more sophisticated our cyber security technology becomes, the more sophisticated cyber criminals become in their attack approaches. It's an escalating war where companies are always playing catch up to the bad guys. Cyber "whack-a-Mole".

What can organizations do to protect themselves?

It is well documented that corporate culture impacts company performance, either positively or negatively. A toxic culture was the culprit behind Wells Fargo employees opening over 1 million fraudulent bank accounts in order to meet management-mandated sales quotas [5]. And the $ 25 billion diesel emissions fraud perpetrated by Volkswagen was the result of a top down culture of hubris and arrogance in a rush to beat Toyota and become the largest global automobile company [6].

By John R Childress
Chairman, PYXIS Culture Technologies

At the other end of the spectrum, a strong "Culture of LUV" [7] has allowed Southwest Airlines to deliver excellent customer satisfaction and post 44 straight years of profitability in a difficult industry.

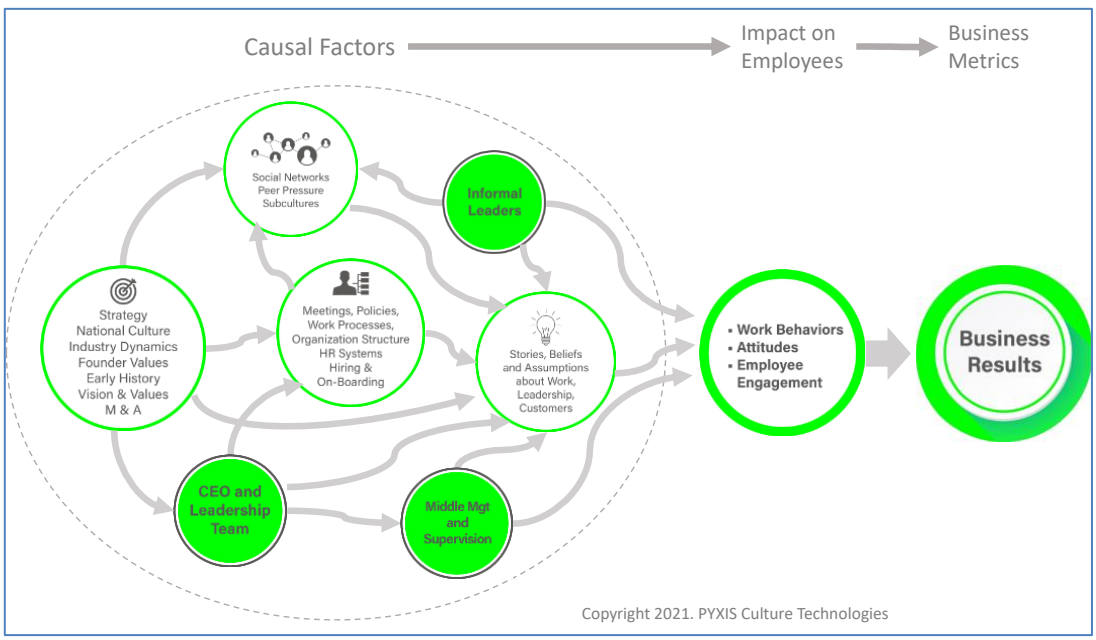


At PYXIS Culture Technologies, we view culture as the missing link in an effective cyber security strategy. A strong cyber security culture can be a highly effective and adaptable bulwark against the growing tsunami of cyberattacks.

So what is cyber security culture and how does it impact cyber security?

Cyber security culture is an interconnected ecosystem of organizational causal factors that influence employee actions and behaviors toward cyber security. Causal factors such as policies, training, onboarding, supervision, physical security protocols, third-party contractors, working from home protocols, password policies, shadow IT and a myriad of other factors interact together to create a work environment (cyber security culture) that either supports good cyber behavior among employees, or allows for cyber security shortcuts and other cyber risky behaviors. It is easy to see how a culture of fear of making a mistake or speaking up can negatively impact cyber security.

This graphic shows how numerous interconnected causal factors impact employee behaviors and business results:

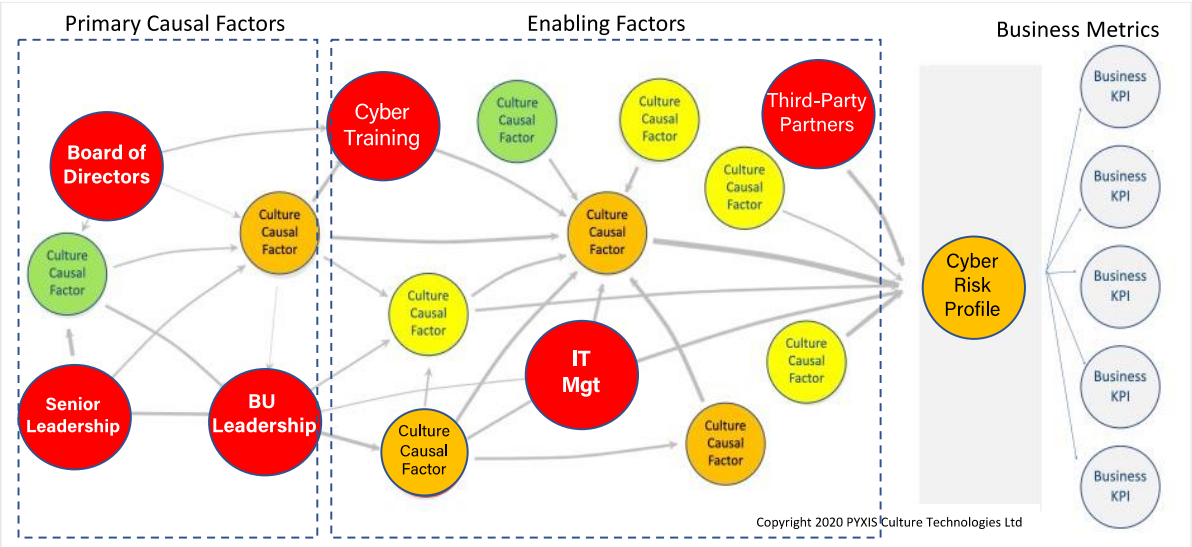


By John R Childress
Chairman, PYXIS Culture Technologies

Building a Strong Cyber Security Culture

The first and most important step in building a strong cyber security culture is to identify the strengths and weaknesses of the many cyber security culture causal factors in your company. Using special ecosystem modelling software and culture analytics developed by PYXIS Culture Technologies, it is possible to use qualitative and quantitative company data and information, as well as a special cyber security culture audit, to build a map of your current cyber security culture.

This mapping approach shows not only which causal factors are strengths, but also helps identify the hidden cyber security risks in your culture For example, here is an example of such a cyber security culture map, with key risks highlighted.



Each of the drivers are color coded from Green to Red, indicating strengths and current risks. A score for each driver is determined from the qualitative and quantitative inputs to our algorithm, and an overall cyber effectiveness score is then created. This analysis also shows how cyber security culture impacts business metrics. In this example, there are several causal factors that need improvement. The map is also divided into what we term Primary Causal Factors and Enabling Factors. Using a built in scenario planning function, we can also model the overall impact on cyber security by adjusting the scores of one or more causal factors.

For example, research has shown that the actions and behaviors of senior leaders are a powerful factor in driving positive cyber security behaviors. Yet we have found that in most organizations there is little active promotion of cyber security during town hall meetings and staff meetings. As a result, employees receive little feedback or coaching for positive cyber security actions, allowing negative peer pressure and demanding project time schedules to drive cyber security shortcuts.

By **John R Childress**
Chairman, PYXIS Culture Technologies

IT management is another strong cyber security driver, especially when IT policies are difficult to implement on a daily basis and the protocols of cyber hygiene are not rigorously implemented. In many companies IT budgets are under constant pressure to be reduced, which negatively impacts the ability of the company to improve their cyber safety since the budget for the Cyber Security function is a part of the overall IT budget.

What Does Your Cyber Security Culture Look Like? Where are the Hidden Risks?

If you don't understand your culture,
you don't understand your busines risks.

About PYXIS Culture Technologies

PYXIS Culture Technologies differentiates itself from the traditional culture and performance improvement consulting firms in two important areas. First, we combine over forty years of experience in studying, researching, and supporting senior leadership teams to understand how culture impacts performance with deep operational experience in culture transformation, digital transformation, and business turnarounds.

We focus on culture as a business issue, not an HR issue. We also believe that internal people are the best to promote and sustain the culture, NOT consultants with off-the-shelf training programs. To this end our methodology is to operationalize culture and transfer cyber safety and culture building skills to in-house teams.

Find out more about PYXIS at www.pyxisculture.com
Or contact: info@pyxisculture.com

References:

1. https://cybersecurityventures.com/cybersecurity-market-report/
2. https://lnkd.in/em6FBt2
3. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
4. https://smallbiztrends.com/2019/05/2019-small-business-cyber-attack-statistics.html
5. https://www.forbes.com/sites/jackkelly/2020/02/24/wells-fargo-forced-to-pay-3-billion-for-the-banks-fake-account-scandal/
6. https://fortune.com/2018/02/06/volkswagen-vw-emissions-scandal-penalties/
7. https://www.forbes.com/sites/jeffthomson/2018/12/18/company-culture-soars-at-southwest-airlines/?sh=67763b66615f

info@pyxisculture.com
contact John R Childress
jrc@pyxisculture.com