pyxis

Cyber Security Culture: Using Analytics to Identify and Mitigate Risk

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

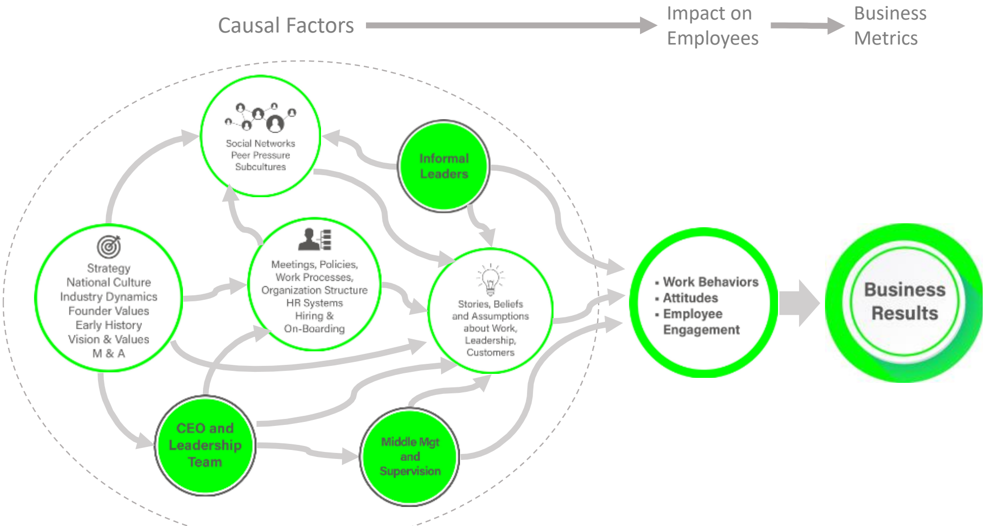
Cyber Security Root Causes:
Using Analytics to Identify and Mitigate Risk

As cyber threats continue to grow, companies are fighting back with technology, phishing campaigns, tougher compliance requirements, and zero trust policies. While these safeguards are important, they are not sufficient. Breaches continue to grow and many involve employee errors and mistakes.

$ 6 T	485%	43%	90%
Cost of cyber crime in 2021	Increase in global ransomware attacks between 2019-2020	Of cyberattacks are against SMEs	Breaches from Human mistakes and errors

PYXIS Culture Technologies spent the past 3 years working with a range of clients to identify the root causes of cyber security. In this effort we have developed a visual systems-modelling approach to identify the drivers of effective cyber security. Understanding the specific root causal factors that impact cyber security allows the Board and C-suite to actively engage in meaningful dialogue into how to improve cyber security. Using our systems modelling approach they can explore best practices, implement targeted improvement projects, and track progress towards effective cyber security. The goal? The Board, C-suite and all employees working together to improve cyber safety across the enterprise.

At PYXIS, we look at cyber security as an interconnected ecosystem, much like the schematic model below.



Copyright 2021. PYXIS Culture Technologies

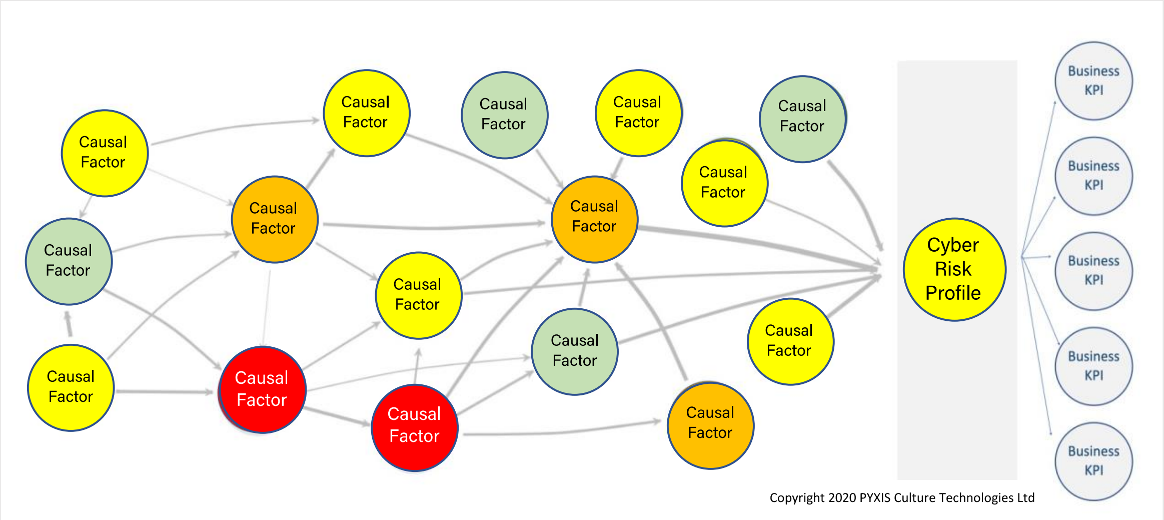
Our research used internal company data from clients in different industries to gain insights into which internal company factors pose the greatest risks to cyber security. Our research also enabled us to build an initial library of cyber security best practices. The result? A unique roadmap and toolkit for building a strong and responsive cyber security culture.

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

Cyber Security Insights

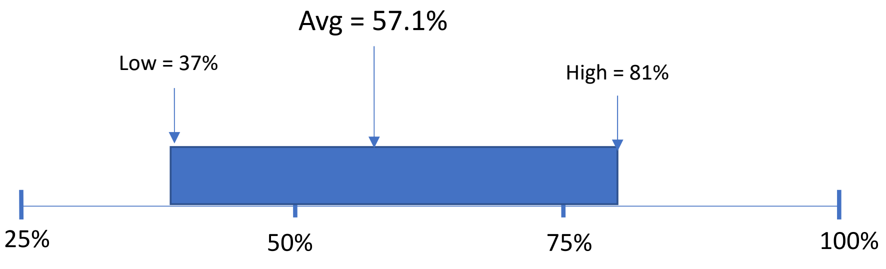
The PYXIS software platform uses quantitative and qualitative company data and produces a color-coded, visual systems map showing the interconnected causal factors and the overall health of the cyber security ecosystem. Each causal factor is made up of multiple data inputs and is scored on a 0-100% scale and color-coded.

Below is an example of an enterprise cyber security map showing how the various causal factors are interconnected and how together they impact business metrics. In this study, we used a generic template system map developed by our team, identifying the common factors in most organizations that have the greatest impact on employee cyber security attitudes and actions. In total we used 121 data inputs which we standardized across all organizations in our study.



Study Results

The average cyber security culture health score from our study was 57.1%, a strong indication that companies are not adequately addressing all the important elements impacting cyber security.



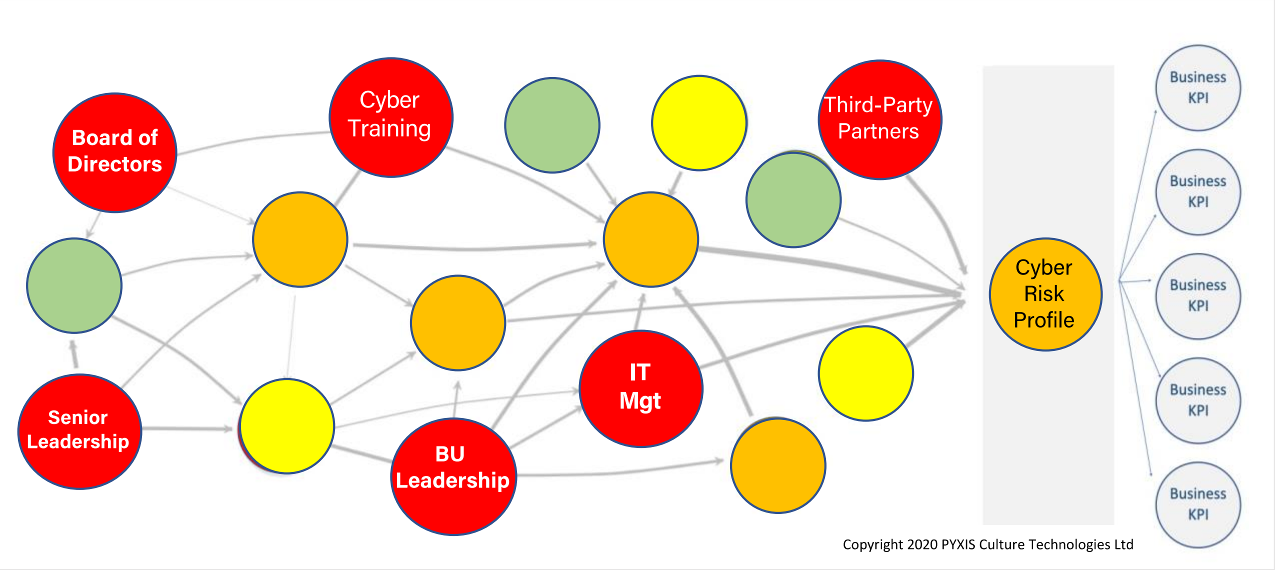
Cyber Security Effectiveness Range

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

A more detail analysis of client data reveals six common elements that create the greatest potential risk to overall cyber security effectiveness

These are:

- Third-Party Partners,
- Senior Management,
- Cybertraining,
- Business Unit Leadership,
- Board of Directors
- IT Management



These low scoring cyber security causal factors impact, in multiple ways, how employees behave and react to cyber security policies, practices and potential cyber risk events. Improving these specific elements can have a significant improvement on the overall effectiveness of an organization's cyber security.

Scenario Planning Using Best Practices

The PYXIS platform has a unique built-in scenario planning function that allows Boards and the C-suite to dig deeper into the data and model specific improvements, based on best practices.

To improve an organization's cyber security effectiveness, our software contains a library of best practices that management can use to explore and implement improvement programs to strengthen the overall cyber security culture.

The ROI of Improved Cyber Security

The PYXIS Culture Management Platform uses historical company data to link improvements in cyber security to business outcomes. This allows management to calculate the potential ROI of one or more improvements. Traditional cyber security business metrics such as:

- Number of Exceptions
- Gross Losses due to Fraud and Breaches
- Number of Recurring Incidents
- Average Duration of Vulnerability
- Employee skills in cyber security

can be linked to specific culture improvements.

Identifying Your Cyber Security Strengths and Risks

While this study shows the combined scores from multiple organizations, insights into your enterprise-wide cyber security effectiveness can be gained from a custom designed visual cyber security systems map. PYXIS Culture Technologies will work with you and selected members of your cyber security team to develop a customized map and assessment you can use to make positive improvements to reduce risk and improve cyber security effectiveness.

> "Cyber security is the fastest growing threat to organizations and society.
> We must work to improve people, processes and culture."
> ~ Stéphane Nappo, 2018 CISO of the Year

pyxis

jrc@pyxisculture.com
pyxisculture.com