pyxis

Cyber security: What’s the missing link?

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

Effective cyber security is a value chain composed of essential links.

On the technology front, the number of threat detection and internal monitoring tools are growing. At the same time, we see growth in regulatory compliance policies and processes, focusing attention on prevention and quick response.

If these elements were all we needed, we would be winning the cyber security war. But we are not. From 2017 to 2018, the number of cyber-attacks rose by 27 percent. Globally, cyber-crime costs around US$600 billion a year and that figure is expected to top US$1 trillion soon. Put simply, technology and compliance can't keep up.

Individual hackers, criminal gangs and nation states target companies as well as political, governmental and social organizations. And it's not just large companies. More and more smaller organizations are being targeted, and they don't have the capital to invest in sophisticated cyber technology. A successful breach can spell the end for a small company.

It's clear that we need another strong link in the cyber security chain.

The answer is culture

It is widely recognized that corporate culture can enable or block strategy execution. The same is true for cyber security. Yet cyber security culture has long been overlooked.

The data clearly demonstrates the importance of cyber security culture:

80%
breaches due to employee error or malicious actions

↑45%
of employees think it's okay to open any email

↑90%
of CISOs say employees are a critical cyber risk

↓24%
of firms have plans to develop cyber security culture

CISCO and Cybersecurity Ventures 2019

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

I believe that standard culture assessments do not provide a true picture of corporate culture. That's because traditional definitions of culture focus on employee behaviors, beliefs and shared values, not causal factors. They do not identify the causes, or drivers, that determine company culture and influence employee behaviors when it comes to cyber security. That's because behaviors, beliefs and values are the outcomes of a culture – not the culture itself.

I define cyber security culture as an interconnected network of work practices and company policies, business processes, goals, management and supervisory actions, leadership focus, peer pressure and employee attitudes. In combination, these elements determine how employees engage with cyber security.

By using analytics to visually map how internal company factors influence employees' behavior, our Culture-as-a-Business-SystemTM model provides CISOs and businesses leaders with deep insights. We map, model and quantify the impact of culture on an organization, revealing hidden cyber risks and identifying opportunities for positive change.

— We use data and metrics to help determine which elements of the culture enable security and which create risk.

— We help employees understand how their work and actions directly impact the health of the company, so they become the organization's "human firewall."

— Our cyber security system map identifies business functions that operate as silos and helps managers integrate them into an effective enterprise solution.

— We pinpoint cost-effective measures to strengthen your cyber security. This is a more targeted and economical approach than standard "culture improvement" workshops.

— Our analytics predict the impact of proposed changes, giving executives the tools to manage culture proactively.

— Our success is measurable. We track the effectiveness of cyber security culture over time and link it to business metrics.

By expanding the CISO's tool kit to include technology, compliance and culture, we can connect the entire cyber security value chain and protect your information, staff and customers from the growing tsunami of cyber-crime.

pyxis

cw@pyxisculture.com
pyxisculture.com