CYBERSECURITY RISK ANALYSIS

Providing your board and executive leadership team with situational awareness of your current cyber risk areas and opportunities for improvement.

△TriCorps

CYBER RISK OWNERSHIP

Board of Directors and executive teams should take responsibility for understanding and establishing the levels of cyber risk their organization can reasonably accept. Cyber risk tolerance is a board level decision because there is potential for significant financial impact, possible regulatory fines and market reputation damage. In the past, executives have abdicated the cybersecurity risk to their IT department. Today, industry best practice is make cybersecurity risk acceptance a board level decision.

BOARD OF DIRECTORS

EXECUTIVE TEAM

CSO, CIO, CISO, CTO

IT DEPARTMENT

BOARD OF DIRECTORS

EXECUTIVE TEAM

CSO, CIO, CISO, CTO

IT DEPARTMENT

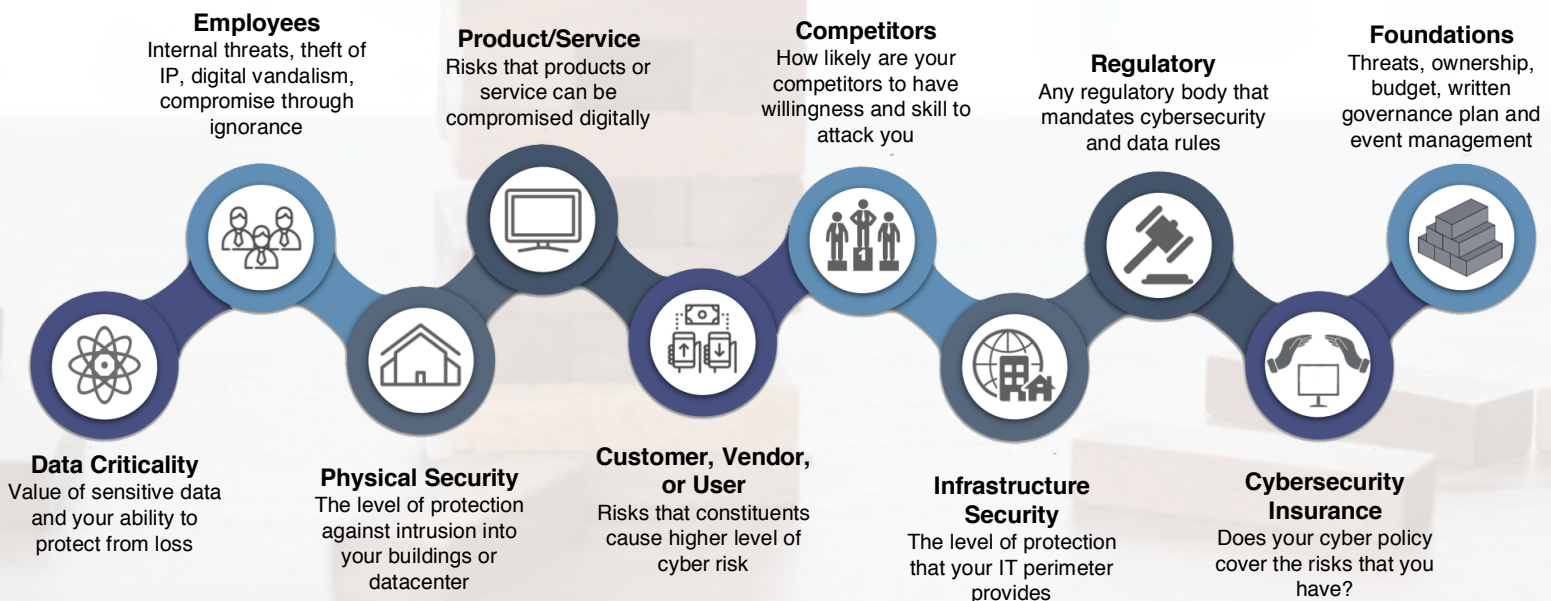Makes bulk of decisions

Makes bulk of decisions

WHAT IS A CYBERSECURITY RISK ANALYSIS?

Risk is composed of two parts: the probability of something going wrong, and the negative consequences if it does. Risks can be difficult to spot and even more difficult to manage. If your organization is hit by a consequence that you hadn't planned for, costs, time, and the reputation of your organization can be on the line. Our cybersecurity risk analysis is an essential tool in helping you identify and understand the risks that your organization faces, by managing these risks, their impact on your organization is minimized.
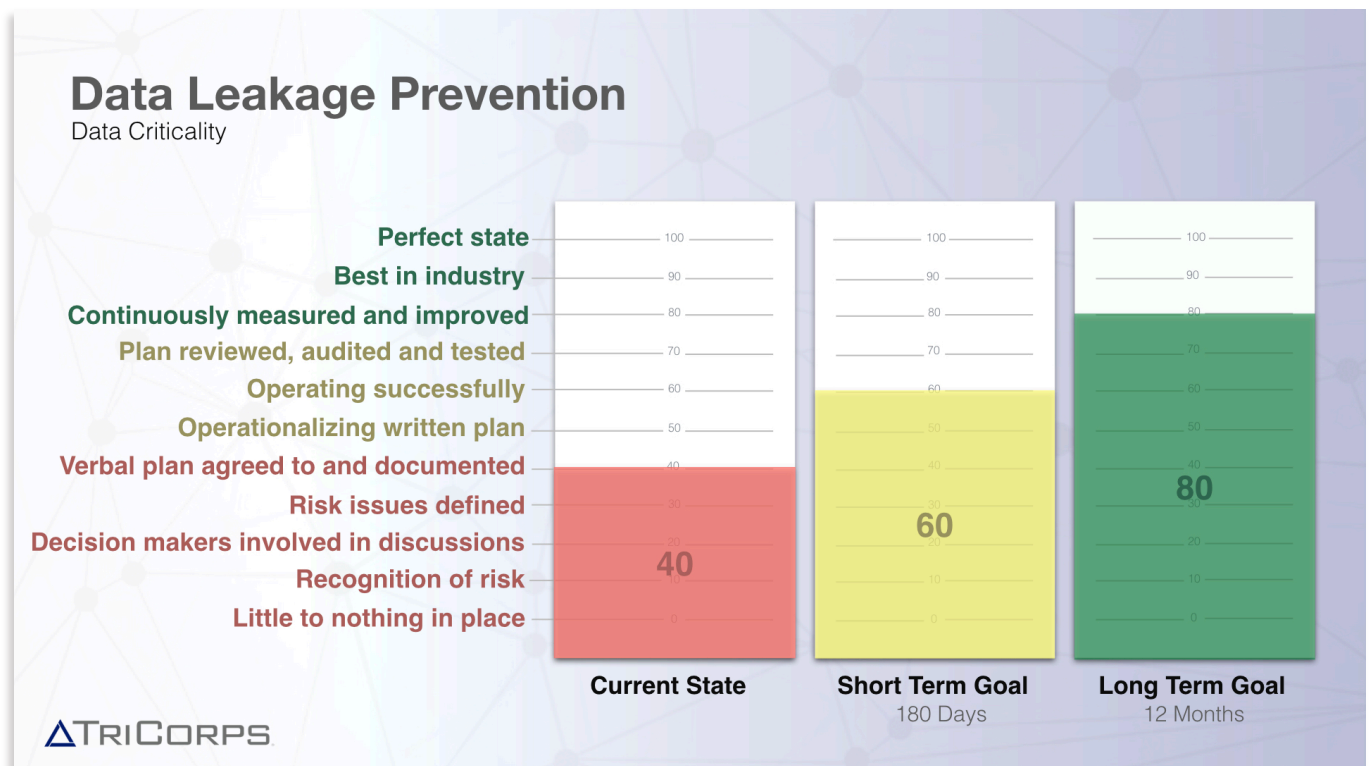
TriCorps provides a third-party analysis of the highest cyber risk areas of your organization. The service will provide your team with a series of complete and concise reports and a single-page summary of our ten critical risk areas and the sweet spot for risk acceptance. We will score the different metrics and help your team determine target scores: for each of the risk areas. In our assessment dashboard, your team can see the current organizational risk and understand potential areas for improvement.

TRICORPS TEN CRITICAL RISK AREAS

Employees
Internal threats, theft of IP, digital vandalism, compromise through ignorance

Product/Service
Risks that products or service can be compromised digitally

Competitors
How likely are your competitors to have willingness and skill to attack you

Regulatory
Any regulatory body that mandates cybersecurity and data rules

Foundations
Threats, ownership, budget, written governance plan and event management

Data Criticality
Value of sensitive data and your ability to protect from loss

Physical Security
The level of protection against intrusion into your buildings or datacenter

Customer, Vendor, or User
Risks that constituents cause higher level of cyber risk

Infrastructure Security
The level of protection that your IT perimeter provides

Cybersecurity Insurance
Does your cyber policy cover the risks that you have?

WHAT YOU'LL RECEIVE

The result is a single-page summary which shows your Risk Tolerance Profile, Current and Target Scores, Gaps, Risk Improvement Actions, Estimated Cost to Remediate and possible negative consequences and penalties (regulatory fines, etc.) of inaction.

Data Leakage Prevention
Data Criticality

	Current State	Short Term Goal 180 Days	Long Term Goal 12 Months
Perfect state			
Best in industry			
Continuously measured and improved			
Plan reviewed, audited and tested			
Operating successfully			
Operationalizing written plan			
Verbal plan agreed to and documented			
Risk issues defined	40	60	80
Decision makers involved in discussions			
Recognition of risk			
Little to nothing in place			

△TRICORPS

For more information, contact us at 405.621.9006
or email us at info@TriCorps.com

△TRICORPS

△tricorps.com   ☎ 405.621.9006   ✉ info@tricorps.com