Technology,
Information
& Security

Next-Generation Cyber Security

collective
insights
CONSULTING

In a world where everything is connected, anything can be disrupted.

69 days

is the average time to resolve malicious insider attacks [1]

69%

of IT security leaders said their organizations have a reactive approach to cyber security [2]

84%

of cyber-attacks are caused by human errors (i.e. easy password, physical devices left unsafe, or failing to apply patches) [3]

If You Answer "Yes" to Any of These Questions:

Q: Has your organization experienced a breach or an attack?

Q: Has your board developed an interest in Cyber Security?

Q: Do you have multiple point solutions for Cyber Security performing similar functions?

Q: Has an audit identified security issues that need to be remediated?

Q: Are you looking to shift identity and access management to the cloud?

Q: Is your organization lacking minimum security standards?

Then our expertise is what you need. Together, we'll reach a better best.

The threat landscape is continuously evolving as adversaries are increasing the sophistication of cyber-attacks through their use of artificial intelligence and machine learning.

The number of potential intrusion points for an attack is increasing as companies embrace emerging technologies to better engage employees and customers, increase the number of endpoint devices, automate their processes, and shift workloads to the cloud.

These trends drive the criticality for today's business to further harden their security posture across the company to stay ahead of threats and adversaries and minimize the risk of exposure.

Our Next-Generation Cyber Security service helps our clients strengthen their security posture to better:

Enable a seamless end-user experience

Protect users' identities and control access to valuable resources

Protect sensitive data wherever it lives or travels

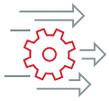Detect incidents using predictive and behavioral analysis

Respond to incidents via automation

Promote best practices to manage security-related risk

Our Services.
Your Success.

Business Transformation

- Strategic Planning
- Target Operating Model Architecture
- Strategic Finance
- Supply Chain Transformation
- Process Optimization
- Enterprise Performance Management

Technology, Information & Security

- Technology Strategy & Architecture
- Cloud & Edge Computing Enablement
- Technology Modernization
- Intelligent Information & Analytics
- Integrated Automation
- Next-Generation Cyber Security

Human Capital

- Organizational Change Management
- Strategic Communication
- Instructional Design & Development
- Workforce Development
- Organizational Design
- Culture Transformation

Operations & Management

- Program & Project Management
- Business Continuity
- Strategic Selection
- Vendor Management
- Mergers & Acquisitions Integration Management
- Portfolio & Demand Management

References

1 Statista, https://leftronic.com/cybercrime-statistics/
2 https://www.cpomagazine.com/cyber-security/it-security-leaders-board-members-need-to-accept-more-responsibility-for-cybersecurity-risk/
3 https://www.computerweekly.com/news/450425184/Security-professionals-name-top-causes-of-breaches

Collective Insights Consulting

info@collectiveinsights.com | www.collectiveinsights.com

3565 Piedmont Road NE
Building 1, Suite 520, Atlanta, GA 30305

© Copyright 2020