Is your approach to security actually protecting you today?

What about tomorrow?
Piecemeal Approaches to Security Put Business at Risk

Three Key Challenges That Arise From a Piecemeal Approach

1. Constantly evolving threat landscape

2. Confusing myriad of security products

3. Costs associated with planning, product, implementation, talent and time

300% increase in the number of security vulnerabilities discovered in the last 5 years.

- U.S. National Institute of Standards and Technology

75 The average number of security products an enterprise uses to secure their network.

“That’s a lot of noise and a lot of monitoring and testing for security practitioners.”

- CSOonline.com

“56% of organizations are addressing the hiring crunch by subcontracting at least some portion of their cybersecurity teams, most often to managed service providers.”

- Sascha Eder, CEO, NewtonX in VentureBeat, October 13, 2021
Are Today’s Product-Focused Approaches Effective?

92% percent of cybersecurity professionals state that IT complexity makes supporting current organizational functions a challenge.

“Check the box” product approaches can leave security gaps.

“One size fits all” security platforms may not align with unique business needs.

“A one-size-fits-all security approach will create areas of too much security and others of too little.”

– Cybertalk.org

– Top 10 Security Projects for 2020-2021, Gartner
Piecemeal Approaches to Security Put Business at Risk

Business Impacts of Getting Your Security Wrong

- **Operational slowdowns**
- **Insurance risks & non-compliance**
- **Business continuity**
- **Negative brand reputation**
- **Financial loss**

### Business Impacts

- **38%**
  The reflected total business share lost in breach costs.
  
  – Cost of a Data Breach, IBM, 2021

- **52%**
  Of consumers would consider paying for the same products or services from a provider with better security.
  
  – Varonis, 2020

- **$4.62m**
  The average total cost of a ransomware breach, minus the cost of the ransom.
  
  – IBM, 2021
A successful security program is built on three key attributes:

- **Scalability**: Scales with your business growth
- **Effectiveness**: Based on your unique risk profile
- **Customization**: Intentionally designed for your business
Augment Your Existing Solutions to Plug Your Security Gaps

An understanding of your current state provides an objective, strategic view to identify security gaps.

**Assess**
Identify gaps in practices, policies, controls, and the security stack that put your customers’ data and assets at risk.

**Recommend**
Provide impartial, standards-based guidance on improving the security program.

**Architect**
Craft a strategy to augment the security program’s capabilities with best-of-breed technology and services.

**Mature**
Implement operational practices and oversight to provide ongoing assistance.

What About My Existing Investments?
Developing a Security Program is a More Responsible Approach

A roadmap for your security program provides high level visibility of your security needs and enables you to strategically prioritize your investments.

Operational Improvements
Insurance & Supply Chain Compliance
Business Continuity
Customer Delight
Financial Gains

Client Satisfaction
“I will definitely recommend this product to any business owner, especially the startups. It gives you the visibility and flexibility without really worrying about the system. CBTS has taken something that’s always been an issue and made it an advantage for the business owners. Their system is never down, and it has great features. Everything business owners are looking for is there and many more that you will find along the way.”

– Grant Mitchell, Principal Owner, PwC Cyber Survey
CBTS is Trusted as an Expert Security Partner

Our certified experts provide a wealth of knowledge around best-of-breed security, bringing experience from working with over a thousand customers, each with specific needs.

Security Capabilities and Offers

- **Security Assessments**
  - Vulnerability Assessments
  - Penetration Testing
  - Application Security Development and Testing
  - Security Program and Architecture Review
  - Virtual CISO
  - Risk Management, Compliance and Governance

- **Cloud Security**
  - Monitoring and Management for AWS and Azure
  - Analytics and Threat Intelligence
  - Cloud Networking Security
  - Cloud Security Posture Management

- **Security Technologies**
  - Application Security
  - Network Security
  - Endpoint and Mobile Device Security
  - Data Security
  - Vulnerability Management
  - Authentication
  - Encryption

- **Managed Security Services**
  - Threat Detection and Response
  - Vulnerability and Patch Management
  - Email
  - Firewall
  - Backup and Disaster Recovery
  - Endpoint Protection
  - Multi-Factor Authentication

“Working with the CBTS team makes it feel like our law firm has an ‘army’ behind it” — Terry C. Duennes, Security Architect, Dinsmore
Next Steps

Schedule a 1-hour meeting with our Security Specialists and your key stakeholders to do a deeper discovery of your security posture.

Let's start you on your path to success today.

cbts.com/security