CIOCoverage

Driven For Technology Leaders

10 BEST

COMPLIANCE

Companies to watch in 2024

Compliance Solutions
Strategies

CSI

Foresite Cybersecurity

Riskonnect Inc.

Artificial Intelligence in
Compliance

Compliance Technology,
Redefined: Embrace the
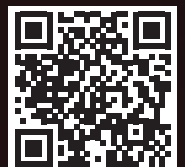Renaissance in Compliance
Management

Key Objectives of Handling
Regulatory Compliance in
Technology

Navigating Healthcare
Compliance in a Dynamic
Landscape: Steadfast
Amidst Change

BUSINESS
CYBER SECURITY
SOLUTIONS

Ron Searle
CEO

BUSINESS CYBER SECURITY SOLUTIONS

10 BEST COMPLIANCE
Companies to Watch in 2024
CIOCoverage

Amid escalating cyber threats, leadership teams grapple with the complex task of safeguarding sensitive data and meeting evolving compliance standards, accentuating the crucial need for effective cybersecurity and compliance solutions. Business CyberSecurity Solutions (BCSS) stands as a pragmatic force that simplifies complexities for leadership teams. The overarching goal is not only to protect organizations but also to navigate the ever-evolving cybersecurity and data privacy compliance landscape.

Addressing current trends impacting the cybersecurity space, BCSS takes on the challenge of expensive and elusive cyber insurance for businesses. With many leaders struggling to navigate complex insurance applications, BCSS offers fractional/virtual Chief Information Security Officer (VCISO) services to guide businesses through the process, ensuring coverage when needed. In a world where breaches are rampant, BCSS serves as a counselling partner for business

Ron Searle
CEO

owners, providing affordable solutions and helping them understand and prioritize cybersecurity measures.

Recognizing the challenges faced by internal IT teams, BCSS offers fractional/virtual CISO and CIO services. This collaborative approach assists IT teams in adapting to the rapid pace of cybersecurity changes and focuses on addressing the big-picture causes rather than micro-issues. As data privacy rules loom, BCSS emphasizes the importance of understanding data from inception to destruction, offering fractional/virtual CISO services to navigate the evolving data privacy landscape.

Engaging with prospects and customers in the compliance and cybersecurity space, BCSS identifies key challenges—most notably, the struggle to start and prioritize cybersecurity efforts, the presence of non-professional IT team members, and the lack of awareness about existing assets pose significant hurdles. BCSS steps in by providing education, solutions, and assistance in communicating risks to the executive level.

A crucial component emphasized by BCSS is in-depth knowledge of the existing infrastructure. Utilizing the NIST Cybersecurity Risk Framework, BCSS underscores the importance of the "Identify" phase. This phase ensures that organizations know what they have, prioritizing the significance of tools like Remote Monitoring and Management (RMM), network monitoring, and asset inventory s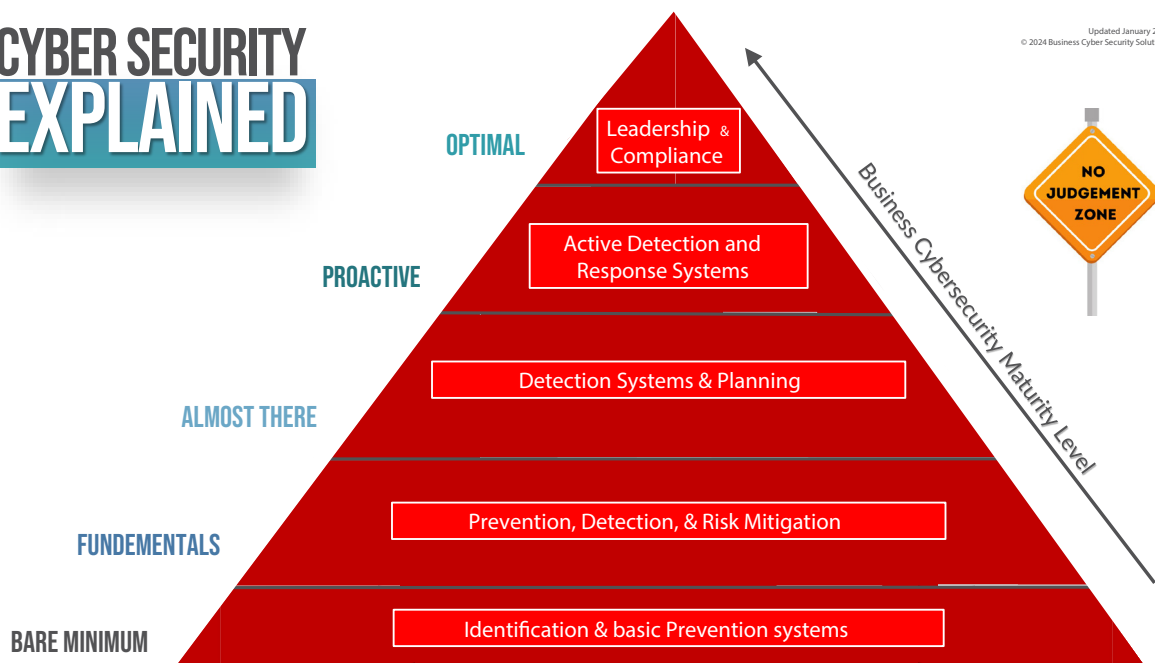ystems. BCSS highlights the vulnerability stemming from untracked devices in growing networks, advocating for robust cybersecurity measures.

BCSS adopts a tiered approach, prioritizing facts over opinions. By understanding industry mandates and gauging the leadership team's risk tolerance, BCSS categorizes organizations into five levels of cybersecurity and compliance. The process begins with in-depth interviews to comprehend the business and industry, followed by the identification of regulatory compliance frameworks. BCSS evaluates existing applications, personnel, and policies, aligning them with compliance frameworks. A GAP Analysis is then conducted to determine the necessary enhancements through a combination of applications, personnel, and policy modifications.

Aside from a Virtual CISO

CYBER SECURITY EXPLAINED

Updated January 2024
© 2024 Business Cyber Security Solutions

OPTIMAL — Leadership & Compliance

PROACTIVE — Active Detection and Response Systems

ALMOST THERE — Detection Systems & Planning

FUNDEMENTALS — Prevention, Detection, & Risk Mitigation

BARE MINIMUM — Identification & basic Prevention systems

Business Cybersecurity Maturity Level

NO JUDGEMENT ZONE

(VCISO), BCSS offers a range of services. These include the Managed SOC service that operates 24/7/365 and provides continuous monitoring, ensuring an immediate response to threats and minimizing identification times. The Managed EDR service offers 24x7x365 monitoring for malicious behaviour, swiftly intercepting potential threats. Additionally, the Cybersecurity as a Service (CAAS) package provides a customized solution encompassing people, applications, and services, ensuring comprehensive cybersecurity and compliance.

BCSS emphasizes a back-to-basics approach in cybersecurity, steering clear of buzzwords and marketing jargon. The decision-making process revolves around evaluating risk, risk tolerance, vulnerability, and associated costs. The team is committed to empowering global companies, serving as the frontline defense against cybersecurity threats. The company believes in focusing on fundamentals rather than relying on buzzwords.

According to BCSS, within the cybersecurity decision-making domain, a systematic evaluation encompasses various components. The primary focus is on assessing risk to determine its significance in the current landscape. If the risk is deemed insubstantial, the allocation of time and resources may not be justified.

Simultaneously, the organization's risk tolerance is a crucial consideration. Startups, characterized by a higher risk appetite, may be more accepting of uncertainties than their mature counterparts. This distinction in risk attitude becomes a pivotal factor in shaping cybersecurity strategies.

Vulnerability is another critical facet, requiring a meticulous examination of an organization's susceptibility to identified risks. If existing mitigations prove adequate, further investments might not be imperative.

Transitioning to decision-making metrics, the cost of action plays a crucial role. This involves a comprehensive evaluation of the expenses required to rectify identified issues, encompassing upfront costs, recurring expenditures, and the formulation of policies.
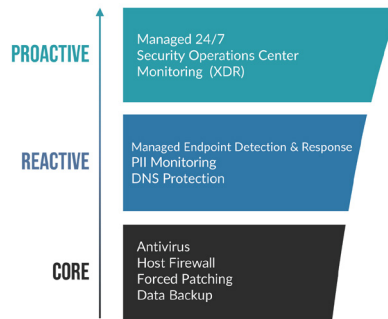
Contrastingly, the cost of inaction unveils the potential repercussions and associated costs if vulnerabilities are exploited. This entails considering not only direct remediation costs but also indirect expenses, legal implications,

EMAIL SECURITY

BEST — **Complete Protection**
Add Backup, Archiving, and Forensics

BETTER — **In Tenant Scanning**
Add AI Based Antispearphishing & business email comprimise detection

CORE — **Inbound Filtering**
Antispam, Antivirus, phishing protection

END POINT SECURITY
WORKSTATION AND SERVER PROTECTION

PROACTIVE — Managed 24/7 Security Operations Center Monitoring (XDR)

REACTIVE — Managed Endpoint Detection & Response PII Monitoring DNS Protection

CORE — Antivirus Host Firewall Forced Patching Data Backup

SECURITY ASSESSMENTS

BEST (QUARTERLY/ANNUALLY) — **Penetration Tests**
Executed by a certified ethical hacker

GOOD (QUARTERLY) — **Vulnerability Scans**
Extensive automated scanning

MINIMAL (MONTHLY) — Network and Security Assessment
Comprehensive automated interla assessments

Want to know more?
847-430-4900 info@businesscybersecuritysolutions.com

and other cascading impacts.

BCSS's impact is evident in case studies showcasing its prowess in overcoming cybersecurity hurdles for clients. The company sets itself apart through its consultative approach, commencing with a complimentary assessment that identifies gaps. Education plays a pivotal role, aiding leadership teams in defining risk tolerance and making informed decisions about cybersecurity and data privacy compliance. BCSS collaborates with customers throughout the journey, managing processes to transition them from their current state to the desired cybersecurity posture. The company's commitment extends to educating executive leadership on the interrelation between IT and cybersecurity.

Looking ahead, BCSS aims to expand its footprint internationally, building on its success in Canada, in 2024. A unique aspect of their expansion plan involves helping Managed Service Providers (MSPs) evolve into Managed Security Service Providers (MSSPs). This collaborative effort ensures MSPs can offer BCSS's product line without extensive research, enhancing the cybersecurity landscape.

BCSS encapsulates its philosophy with a focus on fundamentals. The decision-making process involves evaluating risk, risk tolerance, vulnerability, and costs of action versus inaction. The company is committed to empowering global leaders with knowledge, tools, and teams to safeguard against cybersecurity threats. The emphasis is on education and service, reflecting the team's dedication to being a reliable partner in the cybersecurity realm.

> "
>
> **BCSS prioritizes cybersecurity fundamentals over jargon. Our systematic approach assesses risk, gauges tolerance, and optimizes costs, ensuring our clients fortify their digital defenses with strategic precision.**
>
> **Ron Searle**
> CEO