IndustryWired

February 2022

The **10** Most Trusted **Cybersecurity** Solution Providers in 2022

+ KEY FOCUS AREAS FOR CISOs TO WATCH OUT FOR 2022

NEW ROLES AND OPPORTUNITIES FOR CISOS

BAI SECURITY

Michael Bruck

President/CEO, **BAI Security**

BAI SECURITY

Reducing Cyber Risk For Industries With The Most At Stake

BAI Security is a pure play security assessment firm specializing in providing robust, yet affordable audits for industries with highly sensitive data and critical operations — the same ones most frequently targeted by cybercriminals and most highly regulated by government (bank and finance, healthcare and pharmaceutical, legal, higher education and utilities).

Founded and led by IT expert and Forbes Technology Council member Michael Bruck, BAI maintains a laser-focus on comprehensive security assessments that keep their high-risk clients ahead of fast-evolving cyber threats.

> *"In 2007, I saw a significant gap in the market, where the average organization didn't have access to high quality security audits, nor the luxury of their own IT team. From this concerning place of SMB vulnerability, BAI Security's mission was born — to serve organizations of all sizes with cutting-edge assessments in the most cost-effective manner possible.*
>
> *Fast forward 14 years, and with cybercrime skyrocketing, and organizations financially struggling beneath the weight of a drawn-out pandemic, our mission has never been more relevant."* - Michael Bruck, President/CEO

To guide its innovative trajectory, BAI holds key partnerships with Forbes, Gartner and other cross-industry analysts to anticipate broader market needs, while also listening closely to the realities of current clients to inform new, cost-effective service options.

Michael Bruck

President/CEO, **BAI Security**

Forbes Technology Council

The days of check-the-box audits by generalist firms are over. BAI Security is uniquely positioned to apply the rigor necessary to help high-risk clients detect and correct vulnerabilities, avoid non-compliance fines, and prevent costly breaches. This expertise is what today's security requires.

Michael Bruck
President/CEO, **BAI Security**

Bucking The Generalist Trend

From CEO Bruck's intimate knowledge of the expertise that is required to deliver true depth in assessment, he has long bucked the generalist firm trend of cheap but siloed sub-contractors, instead investing since day 1 in a 100% in-house expert team. BAI's auditors hold impressive credentials and backgrounds. Their continuous collaboration allows them to develop groundbreaking processes that mimic the tenacity of modern-day hackers, putting their client environments to realistic and essential tests.

As Dr. Michele Wilkens, Chief Strategy Officer notes:

"IT security is tied to everything — proprietary data, confidential records, daily operations, worker and patient safety, market reputation, and so much more. There's literally nothing more important for organizational leaders to focus on right now.

But here's the rub — not all security assessment is equal, *and certainly not when it comes to those who do it off the sides of their desks as part of a dozen unrelated services.*

The more highly sensitive the data and more critical the organizational function, the more assessment expertise that's required. Think about it: do you want your surgeon 100% focused on surgery or doing completely unrelated things the majority of their time? Security assessment is who we are and all we do, and that focus is a game-changer for our team and clients in measurable ways."

Peak Cyber Stakes – A Caution For Leaders

For high-risk/high-value asset organizations who are up against today's warp-speed evolution of cybercrime, the team at BAI Security registers weighted concern that vulnerability and penetration testing, compliance auditing, and other security assessment services that should be highly specialized, are increasingly becoming watered-down add-ons for generalist firms and inexperienced start-ups. With outsourced novice auditors and sketchy opensource/freeware tools, such firms can afford to offer bargain basement prices, while claiming to have a legitimate assessment arm that actually only scratches the security surface and leaves organizations vulnerable.

Leaders should take a beat to consider what's really at stake when considering a security partner. Given the ingenuity, breadth and cost of today's security breaches, the problem with a generalist or MSP security assessment is two-fold:

First, if a vendor dabbles in assessment among a dozen other services, the consolidation may feel convenient to decision-makers, but experts suggest such generalists can't possibly stay on top of rapidly developing threats.

As President/CEO Bruck shares:

"The potential consequences of a surface-level and/or less-than-expert audit creates profound risk for partner organizations. Their 'clean' audit could easily lead to a false sense of security, while serious vulnerabilities that could've been found by a more in-depth audit go undetected and unresolved. This creates a very risky situation for any organization given today's climate of aggressive cybercrime. The solution is a truly objective and expert third party — that's what we provide."

Furthermore, no one can objectively 'check their own homework,' according to Dr. Wilkens:

"If a vendor is providing an organization's security or financial solutions, they're pretty unlikely to be as objective as they need to be in rigorously examining and exposing vulnerabilities for the same client to whom they're selling solutions. Only a pure play firm like ours offers the unbiased examination needed to produce trustworthy results."

Thwarting Present-Day Threats

BAI's proprietary assessment methods rely upon four things that many firms today simply don't invest in, but which make a measurable difference in outcomes for BAI clients:

- **Strict use of independently validated, best-in-class tools**: Bruck and team refuse to take the cheap route of open source or freeware, knowing they provide little value and can cause costly false positives. Instead, they exclusively employ globally validated tools endorsed by Gartner Group, Forrester Research, and the like to ensure highly accurate results they can stand behind and clients can trust.

- **Highly skilled in-house experts**: BAI invests in diversely talented professionals with rich backgrounds in vulnerability assessment, social engineering, red teaming, financial and healthcare compliance, and more. While other firms frequently outsource come-and-go auditors, Team BAI builds long-term relationships with clients to learn their distinct environments, while continually innovating cutting-edge methods that simulate present-day cybercrime.

- **A truly exhaustive approach**: By comparison to most audits on the market today, BAI assessments are particularly in-depth and intentionally comprehensive. As President/CEO Bruck explains: *"The vital distinction of our intensive approach provides clients an accurate picture of their security posture, instead of a 'clean report' from a bare minimum assessment that only creates a false sense of security, ultimately leaving issues untended and organizations vulnerable."*

- **Customized, actionable recommendations**: BAI doesn't just hand clients a laundry list of issues or all-too-common generic recommendations; instead, they help organizations prioritize remediation with actionable steps that help them elevate their security posture and better comply with regulations. Dr. Wilkens illustrates with the following: *"It's not always easy for clients to learn their true security picture — prior to partnering with us, they've often been told a surface story that makes them feel good but keeps them in the dark. So, with our comprehensive results, we go an important step further to articulate reasonable ways clients can quickly mitigate risk. When they see this clear path to improved security and compliance, they're 100% on board!"*

Beyond The Regs

BAI Security fully adheres to widely accepted compliance standards (GLBA, SOX, HIPAA, PCI, NERC), as well as best practices per ISACA. However, they also intentionally go well beyond "just the regulations" in their assessments to counter today's aggressive cybercriminals, who well know where most assessment firms leave off.

Offered in fully customizable, à la carte packages to make them affordable for organizations of varied budgets, BAI's current offerings include:

- IT Security Assessment
- GLBA/NCUA Controls Audit
- IT Risk Assessment
- HIPAA Risk Assessment
- Social Engineering Evaluation
- Red Team Assessment
- Network Vulnerability Assessment and Management
- Best Practices Evaluations (Remote Workers, Firewall, Antivirus, Wireless Security, etc.)

Results That Tell BAI's Story

With their innovative proprietary methods, BAI Security achieves impressive results that span technical outcomes, client satisfaction and industry recognition:

- 93% of the time, BAI successfully breaches client environments with their exacting Red Team Assessment.
- 85% of the time, regardless of prior audit by other firms, BAI's IT security assessment reveals serious, previously undetected issues in new client environments.
- Among recently surveyed clients, 100% rated BAI's audit depth & comprehensiveness as "Excellent," along with BAI's deliverables, auditor knowledge, communication, & professionalism.
- **Recent Awards for BAI Security:**
  - 10 Most Influential Leaders in Security — CIOLook, 2021
  - CEO Michael Bruck appointed to Forbes Technology Council — Forbes, 2021 & 2022
  - 10 Best Security Leaders — C Level Focus, 2021
  - 10 Best Security Solutions Providers — IndustryEra, 2020

"They go out of their way to be helpful, offering their guidance and suggestions (as opposed to a cookie-cutter approach). Initially, we chose BAI because of their reputation. We went back to them the next few years because of their people and their professionalism, the depth of their technical and procedural knowledge, and friendliness."

- IT Director & BAI Client, Illinois

The Security Audit Horizon

Looking to the future, the team at BAI Security knows what will empower their clients most centers around providing **trend data** (to see the impact of security improvement efforts while informing ongoing investments), **enterprise-level customization** (to serve specific environments, security challenges and operational goals) and **flexibility** (to address emerging threats while maximizing RO(S)I). To this end, Bruck and team are committed to their original mission of high quality, affordable assessment services, while increasingly weaving in multi-year visibility and responsiveness to the ever-changing security landscape.