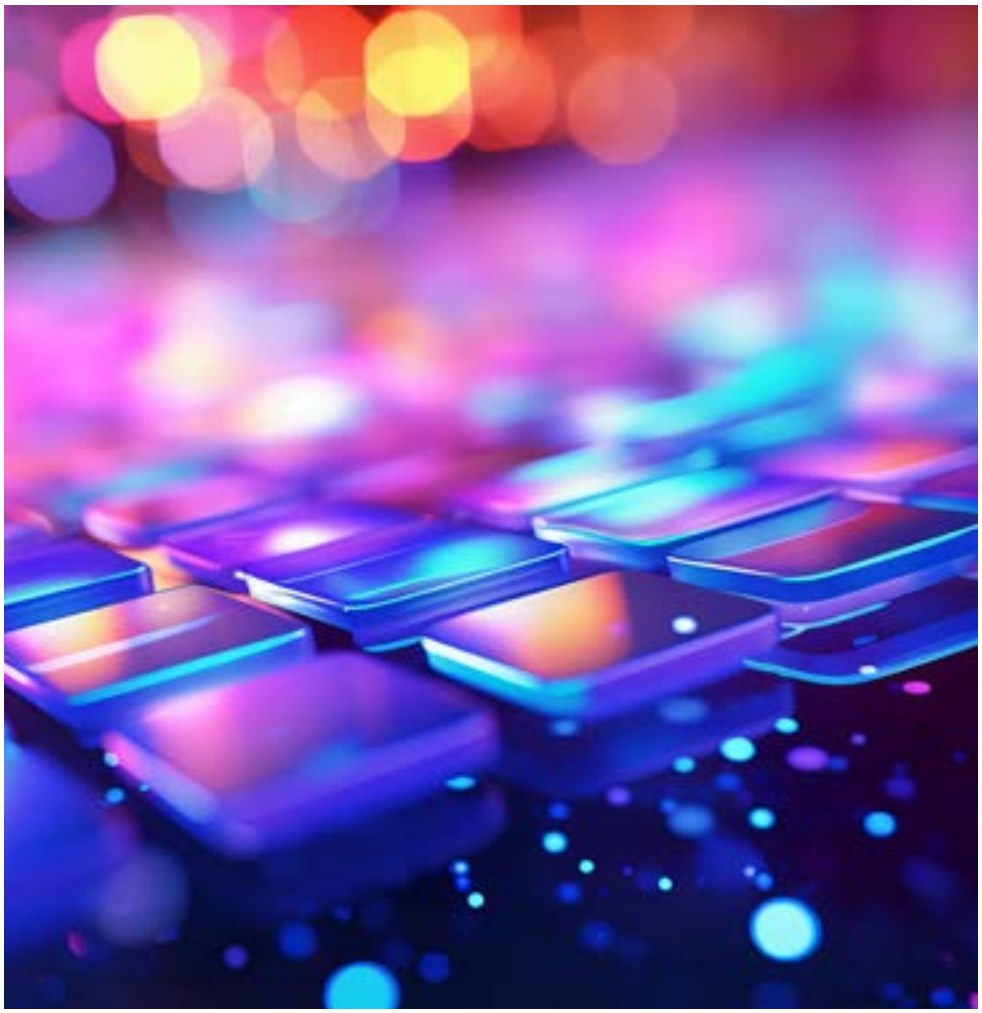
MARINER



Cybersecurity
Is Your Next Smart Business Move

ebook

In today's digital age, where technology evolves at breakneck speed and cyber threats are a given, cybersecurity is not just timely; it's imperative–and it could change how you see your business's future.

That's because cyber threats aren't simply an IT problem anymore; they're a challenge and an opportunity for savvy business leaders.

So, we created this eBook to start the conversation about cybersecurity as a winning strategy.

David Baxter
VP, Marketing

The Heart of the Matter:
VAPT – A Game Changer

Nearly

90%

of technology professionals detected significant risks in their software supply chain in the last year.

Security Magazine / The ReversingLabs Software Supply Chain Risk Survey

Let's talk about VAPT

Vulnerability Assessment and Penetration Testing

Think of it as a health check-up for your business in the digital age. It shows you where you're strong, where you're vulnerable, and how to fortify your defenses.

But here's the kicker: it's also one of the most underrated enablers of growth and a real competitive advantage.

VAPT: An Unsung Hero of Business Strategy

Why does VAPT deserve a spot in your strategic arsenal?

Well, it's simple:

Business Continuity

Imagine your operations humming along smoothly, no matter what digital gremlins try to throw your way. That's the peace of mind VAPT offers.

Compliance and Reputation

In a world where "regulation" is the watchword, VAPT keeps you on the right side of the law—and public opinion.

Competitive Edge

When customers choose who to trust, showing them your cybersecurity chops can tip the scales in your favor.

Supply Chain Confidence

Your customers want to do business with a company that offers a strong, secure link in the line of value creation.

Peace of Mind

There's nothing quite like knowing you've done everything to protect your digital domain, limiting the opportunity for cyber threat impacts on your business. VAPT gives you that assurance, letting you sleep much easier at night.

98%

recognized that software supply chain issues pose a significant business risk.

70%

of companies confirm that current application security solutions fail to protect [them] from software supply chain security risks.

Security Magazine / The ReversingLabs Software Supply Chain Risk Survey

Identifying Your Digital Crown Jewels*

The Power of Knowing

Knowing what to protect is just as crucial as knowing *how*.

It's about asking the right questions: Which assets are vital for your day-to-day operations? What data, if lost, would be a nightmare scenario? It's a strategic exercise, pinpointing where your cybersecurity efforts will have the most significant impact.

From Insights to Impact

Beyond the Vulnerability Scan

Discovering vulnerabilities is one thing; acting on them is where remarkable impact happens. Regular VAPT cycles not only tighten your defenses but also foster a culture of security awareness across your organization. It's about turning insights into actions that fortify your business against digital threats.

Common Pitfalls: More Than Just Technical Glitches

You'd be surprised how often the basics can trip you up. Outdated software, weak passwords, and overlooked security settings are open invitations to cybercriminals. Addressing these vulnerabilities is a progressive step towards a more secure business.

4 Vital Vulnerability Insights to Build Cornerstone Cybersecurity Diligence

Some of the issues we often find in a VAPT that can seriously impact your organization include:

Daniel de Castro, PhD
OSCP, OSWE, OSEP, OSED, OSCE3, OSWP, CISSP
Security Practice Manager

Outdated Software

Lack of a robust vulnerability and patch management program can lead to outdated software, including operating systems, applications, software components/libraries, and even the firmware of networked devices, such as cameras , Wi-Fi access points, and printers, etc.

Outdated software may have known vulnerabilities that attackers can exploit to get a foothold in your organization.

In cases where you cannot update your software, additional controls must be in place to prevent attacks from being successful.

Unvalidated Input

Improper input validation can lead to several kinds of vulnerabilities in your application. Those include buffer overflows, notably on binary applications; code injection, including SQL Injection attacks; Cross Site Scripting (XSS); Cross-Site Request Forgery (CSRF), and, sometimes, even the ability of an attacker to upload malware and execute code on your servers.

Your application must always validate any user input, particularly on the server side. While client-side testing may reduce traffic by ensuring that the data is what is expected, proper and robust server-side validation will prevent an attack even when the client-side protection fails.

Weak Authentication and Authorization

Several kinds of vulnerabilities may allow an attacker to access an application, device, or data that should not be accessible.

These vulnerabilities include default or weak passwords in applications and devices, lack of multi-factor authentication, and improper access controls. All of these can lead to unauthorized access.

Mechanisms such as password resetting/recovery and user management must be tested to avoid account takeovers or an attacker's ability to increase their privilege level.

Security Misconfigurations

Poorly configured security settings (including the use of default credentials mentioned above), the use of unnecessary services, and exposed sensitive information can all be exploited by attackers.

Busting Myths with Reality: Cybersecurity Edition

Let's bust a myth right now: "We're too small to be a target."

The truth?

Every digital footprint is on someone's radar. It's not about the size; it's about the opportunity for attackers.

And here's another: "Our IT team has it covered."

Cybersecurity today needs specialized skills, external perspectives, and ongoing vigilance. It's a whole new ballgame.

From Awareness to Mastery: Your Cybersecurity Impact Journey

Embracing VAPT is a great step on your journey from cybersecurity awareness to business impact mastery. It's not just about ticking off a checklist; it's about adopting a proactive, strategic approach to protect and propel your business in the digital landscape.

Mariner: Your Ally in the Cyber Battle

This is where Mariner comes into the picture. Think of us as your cybersecurity co-pilots, guiding you through the complexities of protecting your digital assets. Our holistic approach blends technology, strategy, and a deep understanding of the human element to fortify your business against cyber threats.

A Call to Action for the Forward-Thinking Leader

If there's one takeaway, it's this: cybersecurity is not a back-office concern but a real business driver. Cybersecurity is no longer just about protection; it's about progress, and it's a powerful tool for business growth, customer engagement, and market leadership.

As we wrap up, I hope this has sparked a new perspective on cybersecurity for you. It's time to move beyond fear of cyber threats to a position of strength, where cybersecurity is part of your brand, a marker of your commitment to excellence and trustworthiness, and a true differentiator.

Cybersecurity Takes a Team

The journey to cybersecurity excellence is not a solo trip; it's a collaborative process.

Partnering with an expert like Mariner means you don't have to navigate this complex landscape alone. We bring the expertise, the insights, and the solutions to help you transform cybersecurity from a challenge into a strategic advantage.

Recognizing VAPT is just the beginning of any cybersecurity journey; the next step is turning insights into strategies and vulnerabilities into strengths. It's about making cybersecurity a cornerstone of your business strategy, a key to unlocking your full potential in the digital age.

Ready to make cybersecurity your next smart business move?

T / (888) 240-9333
www.marinerinnovations.com

Let's Connect

Mariner is an innovation firm that provides core IT and strategic advisory services. We offer a full spectrum of security services, scalable to meet the needs of any organization, no matter your size or sector.

Our approach is also tailored to your business advantage when designing or enhancing foundational Security Resiliency Programs (SRP), as it focuses on defining and monitoring measurable security resilient outcomes to protect revenue and ensure business continuity.