Vata website copy — Developer and notes version — © Vata 2019

‘Off-page’ SEO copy

The copy that shows up in the search engine results. Use the Yoast SEO Wordpress plugin to specify these particulars.

Title:

Vata | Boutique cybersecurity company | Penetration testing and more

Meta description:

Want to protect your business and clients from cyber attacks? Our services include penetration testing, security architecture, cloud security and DevSecOps

URL:

www.vata.net.au

On-page copy

What readers will see on your page when they visit your website.

Above-the-fold copy

This is the first impression — the copy that visitors see before they scroll down the page.

DEVELOPER: The headline should be emphasised over the sub-headline. The call-to-action should clearly be a button and should stand out (while still matching Vata’s colour scheme). Please ensure this is the only text that the visitor sees before scrolling (on all devices). A background image or video that demonstrates protecting clients from cyber threats would be ideal.

Headline:

Protect your business and clients from cyber attacks

Sub-headline:

When you deal with emerging technologies, Vata provides innovative and efficient end-to-end cybersecurity services to tackle any enterprise-level challenge.

Call-to-action button:

Schedule your free consultation <calendar booking link>

Section 1: Problems we solve

Body:

Do you cringe at the time you spend trying to prevent a cyber attack on your business? Does the complexity of your business's cybersecurity challenges feel overwhelming? Are you frustrated that some cybersecurity consultancies can't handle your unique cybersecurity challenges? Does the thought of having to respond to a cyber attack make you sweat? If you answered 'yes' to any of these questions, Vata is the cybersecurity company for you.

Heading 2:

Protect your business from cyber attack

Body:

Cyber attacks are one of the top five global risks in terms of likelihood and one of the top 10 global risks in terms of impact. In the Asia-Pacific region, 64% of businesses that suffered a data breach lost more than USD500,000 as a result — 51% lost more than USD1 million. A whopping 25% of Australian small and medium businesses have been targeted by a cyber attack and the number of cybersecurity incidents is increasing by 33% each year. Our cybersecurity consultants can protect your:

Heading 3:

Commercial secrets

Body:

Innovative business ideas, business plans, financial records, marketing plans, private intellectual property, product designs, patent applications and employee records — if a criminal stole or compromised any of this information, how would your business be affected? A minor loss of some of this information could be expensive, but a major loss could shut your business down for good — or worse. Our cybersecurity services can help you protect your sensitive commercial assets and keep your business safe.

Heading 3:

Finances

Body:

Managing cash flow remains a top concern for Australian small businesses. But if you think everyday cash flow challenges are difficult to overcome, imagine how much harder things could get if your business's financial accounts were compromised during a cyber attack. Running a small business can be tough but our cybersecurity consultants can make running your business that little bit easier by taking care of your cybersecurity measures.

Heading 3:

Customer and client data

Body:

Your customers and clients are the heart of your business. So imagine the disruption it would cause if you lost all their data in a cyber attack. On top of that, if you're not adequately protected, criminals could steal your clients' personal information, breaching their privacy and, in some cases, enabling the attackers to commit identity fraud or theft. How long would it take you to recover from that kind of reputational and operational set back? Days, weeks, months? Our cybersecurity consultants can protect you from such cyber attacks so you never have to find out.

Heading 3:

Reputation

Body:

Your business's reputation is a vital part of your success, so no doubt you strive to shape and protect your reputation in every business activity you do. But while you can control how you and your employees shape your brand's reputation, you've got no control over how competitors and criminals might attempt to tarnish it. You can, however, protect your business from cyber attacks that directly impact your reputation and our cybersecurity consultants can help you do so.

Call-to-action button:

Chat to one of our account managers to learn more

Section 2: Risks we defend against

DEVELOPER: Note, this section is intended to fall under the previous level 2 heading. It's up to you whether you want to change the background etc. to differentiate it from the above section or add interest etc.

The number of ways a cybercriminal can attack a business is staggering. Here at Vata, we can help you protect your business and clients from the full range of cyber attacks. We'll make sure you've implemented the mitigation strategies outlined in the Australian Cyber Security Centre's 'Essential Eight' advice and go beyond those strategies to protect you from the threats that are most relevant to your business. Some of the most common risks include:

Heading 3:

Cloud services risks

Heading 4 / Keywords

Misconfiguration, poor design, missing security controls, shadow-it, third-party security

Body:

Cloud services are a popular way of storing, managing and processing valuable business data, including passwords and customer personal information. That also makes them popular targets for cyber attacks. If you store or backup information in the cloud, through Amazon Web Services (AWS) for instance, cloud security should be a vital part of your cybersecurity program.

Heading 3:

Application Risks

Heading 4 / Keywords

OWASP TOP 10, vulnerabilities, zero-day vulnerabilities and exploits, viruses, ransomware and other malware

Body:

Applications drive the business world today. But each application you rely on may expose your business to vulnerabilities that attackers can leverage. As a result, managing a corporate portfolio of off-the-shelf software and tailor-made applications often complicates the task of maintaining effective cybersecurity measures. Having a sound application security strategy, educating your developers and performing regular penetration tests and code reviews will protect you from unique vulnerabilities that could be introduced to your business by any application. Application white-listing, continuous vulnerability scans, advanced endpoint protection and an intrusion prevention system (IPS) can protect your business from malware and other cyber threats. In addition, if your systems have already been compromised by a cyber attack, we can help you mitigate the incident and quickly recover from it.

Heading 3:

The human factor

Heading 4 / Keywords

Phishing, scams, fraud, embezzlement, internal threats

Body:

Phishing and other kinds of scams remain popular methods of conducting cyber attacks because they're easy to use and are effective tools for fraudulently obtaining sensitive information. But not all cyber attacks come from the outside. 'Inside jobs' like embezzlement and other internal threats are also common and the effects of such attacks can be just as devastating.

All businesses are susceptible to these kinds of attacks and there are two main ways of preventing them. We can put in place technical controls that protect against these types of cybersecurity threats. We can also educate your personnel about everyday practices they can implement to help them identify insider threat indicators and reduce the chances of them succumbing to the sophisticated scams and other cyber attacks used by today's innovative cyber criminals.

Heading 3:

Increased interconnectivity — the internet of things (IoT)

Heading 4 / Keywords

IoT management, Hardware Security Module (HSM), cryptography

Body:

Smart appliances, point-of-sale devices, screens and projectors, wearable devices (like the Apple Watch), automatic lights, surveillance cameras — all kinds of everyday objects are increasingly being connected via the internet but they often lack security features. If you or your business use any of these kinds of technologies, you need protection from network intrusions.

Heading 3:

Denial of service attacks (DOS and DDOS)

Heading 4 / Keywords

DDOS, DOS, CDN, resiliency, syn flood, http get attack, floods, volume attacks, protocol attacks, application attacks

Body:

Denial of service attacks (DOS) and distributed denial of service attacks (DDOS), come in many shapes and forms. The most common type is a DDOS attack, where multiple network resources are used to bombard your system with so much data that it becomes overwhelmed and cannot provide an adequate level of service. With a DDOS attack, criminals can target your website or any system that's connected to the internet and these kinds of attacks are very common. We can develop strategies and tools to help you prevent and recover from many advanced DOS attacks.

Heading 3:

Advanced Persistent Threats (APTs)

Heading 4 / Keywords

Reconnaissance, brute force, phishing, spear phishing, state sponsored, social engineering

Body:

Perhaps the scariest cyber attacks are those that go undetected for prolonged periods of time. An attacker who gets a strong, undetected foothold in your system or business has a lot of time to steal more data, develop more sophisticated ways to do harm, and hack additional parts of the system. Time is always a differentiator in performing an attack, and attackers expend a lot of effort and many resources to quietly gain and maintain access to a network — in fact, cybercriminals often develop bespoke attack methods that are customised to the target. As such, your business will have an increased risk of these threats if you deal with high-value information — businesses in the finance, defence and manufacturing industries are particularly attractive targets. The advanced techniques used to carry out these attacks make it difficult for businesses and even cybersecurity professionals to detect APTs. Our best-in-class, enterprise-level security architects have the ingenuity and drive required to detect and excise existing tailor-made APTs and prevent future attacks.

Call-to-action button:

Request a meeting to discuss the biggest cybersecurity threats to your business

Section 3: Our services

Heading 2:

Cybersecurity consulting — Our services

Body:

Our certified cybersecurity consultants offer a range of services to suit your business's risk profile and budget. Other consultants will just implement the Australian Cyber Security Centre's 'Essential Eight' baseline cybersecurity mitigation strategies. But we do so much more than that. We'll protect your business from the most likely and most damaging cyber attacks so you get the best value from our services.

While we'll tailor our services to your needs, here are the most common types of services we provide:

Please note: Hemed has stated that this will be written in-house. Below I've suggested the main keywords that would be useful in each section that was identified in the Website Brief at the time of writing. These are not included the other two versions of this copy.

- **Managed Services** - Virtual CISO, cybersecurity consultants
- **Security testing** - penetration testing, security assessments, vulnerability scans, code reviews
- **Security design and architecture** - security architecture, cloud security, DevSecOps (you might consider also including DevOps security)
- **Turnkey solutions**
  - **Secure Development Lifecycle** - DevSecOps
  - **Software Defined Data Centre Security** - security architecture, DevSecOps, penetration testing

- **Hybrid cloud security** - cloud security

Call-to-action button:

Request a meeting to explore which services are right for your business

Section 4: Target audience

Excluded from this sample for privacy reasons

Section 5: Why Vata

Heading 2:

Vata — A cybersecurity consultancy with the skills and expertise you need

Body:

You're probably wondering why you should choose us. Here are just five reasons.

Heading 3:

Intelligence, ingenuity, drive

Body:

When you're working on new technologies or innovative solutions, the last thing you want is a cybersecurity consultancy that provides the same solutions to all its clients. We're not like that. Our clients often ask us to map out and define their risks for a unique situation or system. Only once we have a clear picture of your unique risk profile will we develop a custom solution that exactly matches your cybersecurity needs. Why settle for a company who only has hammers when we've got a full toolbox? Our cybersecurity consultants are intelligent, creative and get a buzz out of exploring and tackling unique risk profiles.

Heading 3:

Best-in-class, enterprise-level security architects

Body:

No matter the size of your business, you deserve best-in-class cybersecurity

measures. Our security architects have many years of experience in some of the most demanding security environments including finance, government and defence. Coupled with our knowledge of cutting-edge information security best-practices and a broad spectrum of technologies, this enables us to deliver enterprise-level cybersecurity services to all our clients.

Heading 3:

Excellent customer service

Body:

How many times have you engaged a tech company staffed by experts that resemble the systems they work with — you'd swear they were robots right? Everyone in our consultancy is personable and collaborative. We'll work with *you* not just on your systems and we'll work with any person on your team at any level of your business. We care about your experience with us as much as we care about your business security.

Heading 3:

Better value

Body:

'Cheap' is often a dirty word. And we know you can't afford cheap security that leaves your business vulnerable to highly damaging cyber attacks, especially given the financial pressures faced by all businesses in the current market. But we also know you don't have the massive budget that every big corporation has. That's why we focus on the services that will have the biggest effect on reducing your cybersecurity risk, ensuring you're protected at a lower cost.

Heading 3:

A local team

Body:

When you work with us, we'll assign local account managers and consultants to your project and they'll lead every task.

Heading 3:

Quality assurance

Body:

Every service we offer is backed by our quality assurance — we'll work with you until you're satisfied.

Heading 3:

Internationally recognised consultants

Body:

We have a diverse network of internationally recognised cybersecurity professionals who can handle any task, including:

- Specialised Red Teaming (cyber attack simulation)
- Hardware and automotive hacking
- SecOps
- Security automation
- Public key infrastructure (PKI)

Heading 3:

Certified cybersecurity consultants

Body:

And, of course, our consultants hold top-of-the-line certifications so you can be confident we know our stuff. Certifications our consultants hold include:

- Certified Information System Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certificate of Cloud Security Knowledge (CCSK)

Schedule your free consultation now <calendar booking link>

Section 6: Who we are

Heading 2:

Who is Vata?

Body:

Vata grew out of a need for cybersecurity consultants that could provide quality end-to-end solutions. Our founders, Hemed and Mike, both worked for large organisations that repeatedly experienced issues when outsourcing cybersecurity work to third parties. The solutions offered by most cybersecurity consultancies were often outdated, irrelevant or missing vital components. Sometimes, consultants couldn't offer a solution at all. And even when they could, they often treated deadlines as rough guidelines. The number of contracted suppliers was minimised in an attempt to limit the risk, but Hemed and Mike often had to compensate for the lack of specific skills offered by even the best cybersecurity contractors available.

Recognising that organisations, especially small and medium businesses, startups, fintech businesses and financial services providers, needed quality cybersecurity services but couldn't afford to hire multiple consultants, Mike and Hemed set about building a cybersecurity consultancy that could provide the full range of services in the most cost-effective way.

Today, Vata is a trusted provider of bespoke, end-to-end cybersecurity services. In Sanskrit, 'Vata' means 'banyan tree'. And just like the columns of the banyan tree, Vata will support your business and help you grow by protecting you from the cyber attacks that could otherwise reveal your valuable commercial secrets, decimate your finances or irreparably damage your reputation.

Section 7: Testimonials

Heading 2:

What others say about Vata

Testimonials:

PLACEHOLDER — to be completed when you've received some testimonials.

Section 8: Our clients

Heading 2:

Businesses with spot-on cybersecurity

Body:

We've worked with a wide range of clients both big and small, each with a unique problem set and risk profile.

DEVELOPER: Please insert here the logos of the most prominent clients Vata has helped — where you have permission to do so, of course.

Call-to-action button:

Request a meeting to explore how we can help protect your business from cyber attacks

Section 9: Contact us

Heading 2:

Get in touch now

Heading 3:

And learn how Vata's cybersecurity consultants can start protecting your business's reputation, finances, data and commercial secrets from cyber attack today.

DEVELOPER: It'd be great if you could add appropriate icons next to each contact method below (e.g. a phone for the phone numbers and an envelope for the email addresses). I'm envisaging this in two columns with the contact form on the right and everything else on the left.

Body:

contact@Vata.net.au

+612 9160 6411

Heading 4:

Contact form

Body:

Name:

Email:

Phone number:

Would you prefer we contact you via email or phone? DEVELOPER: I recommend using tick boxes here — 1 each for email and phone and a third for either

If you would prefer a call, what time of day suits you best? (Please also let us know what time zone you're in)

How can we help you?

Break then **Body** (DEVELOPER: I suggest using a different background or other stylistic device to separate this text from the contact form.)

Not based in Australasia? Get in touch with one of our other offices <link to a pop-up that lets your reader choose which of your websites is most appropriate for their location>.