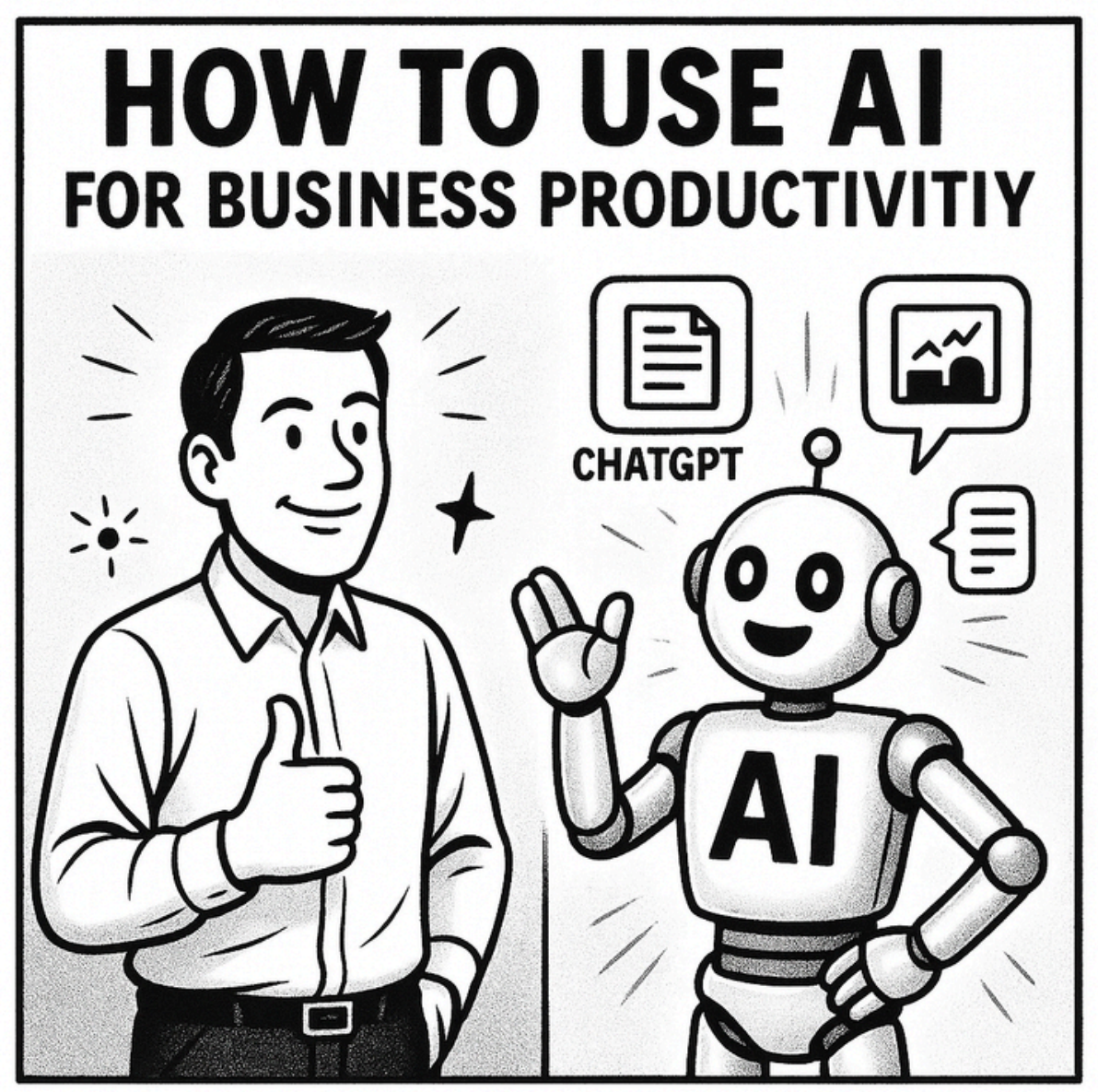
TECH TALK MONTHLY



Inside:

What's Inside

Dear Business Owner 👋

You might think your most valuable business assets are your client list or your brand reputation, but utilizing new AI tools without proper security can compromise all of them in minutes.

Artificial intelligence is no longer a futuristic concept, it's an invaluable tool that boosts efficiency for businesses of all sizes, automating tasks from data analysis to customer service.

While AI adoption is vital for staying competitive, this productivity boost also comes with a significant drawback: an expanded attack surface for cybercriminals. AI models require data, and sending sensitive customer or financial information to a third-party tool can easily lead to data leakage.

The central challenge is figuring out how to harness AI's power while establishing a secure, layered defense. You can mitigate these risks by taking relatively straightforward steps: establishing clear AI usage policies, choosing enterprise-grade platforms that promise not to use your customer data for training, and adopting role-based access controls to segment sensitive data access.

Productivity without proper protection is a risk you can't afford. For expert guidance and a personalized plan to safeguard your business while leveraging AI, contact us today at email@yourcompany.com.

Tony Loffi-Lara
CTO, Oasis Technologies, Inc.

DID YOU KNOW ?

The First AI Program Was Written in 1951: Christopher Strachey wrote a checkers-playing program for the Ferranti Mark 1, one of the earliest computers.

GET IN TOUCH

405.0948.6500

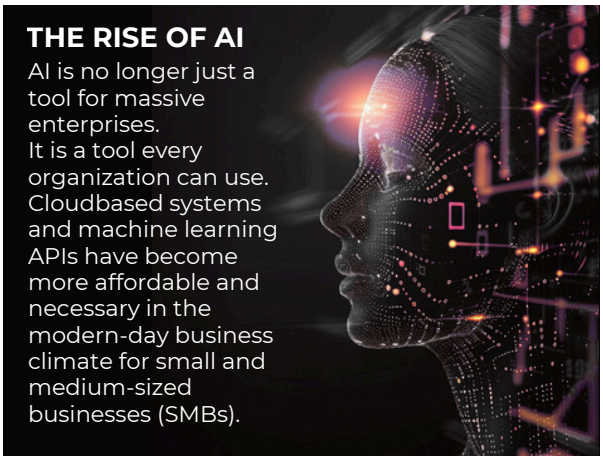
oasis.tech

info@oasis.tech

HOW TO USE AI FOR BUSINESS PRODUCTIVITY WHILE STAYING CYBER-SECURE

Most organizations have realized that AI is not a sentient system looking to take over the world, but rather an invaluable tool. They have come to utilize it to improve their productivity and efficiency. AI solutions have been installed at an astounding rate. Some are used to automate repetitive tasks and to provide enriched data analysis on a previously unrealized level. While this can certainly boost productivity, it is also troubling from a data security, privacy, and cyber threat perspective.

The crux of this conundrum is how the power of AI can be harnessed to remain competitive while eliminating cybersecurity risks.



AI has become common in the following ways:

- Email and meeting scheduling
- Customer service automation
- Sales forecasting
- Document generation and summarization
- Invoice processing
- Data analytics
- Cybersecurity threat detection

AI Adoption Risks

Organizations must understand that implementing any new technology needs to be done with thoughtful consideration of how it might expose these various threats.

• **Data Leakage**
In order to operate, AI models need data. This can be sensitive customer data, financial information, or proprietary work products. If this information needs to be sent to third-party AI models, there must be a clear understanding of how and when this information will be used.

• **Shadow AI**
Many employees use AI tools for their daily work. This might include generative platforms or online chatbots. Without proper vetting, these can cause compliance risks.

• **Overreliance and Automation Bias**
Many users consider AI-generated content to always be accurate when, in fact, it is not. Relying on this information without checking it for accuracy can lead to poor decision-making.

Secure AI and Productivity

The steps necessary to secure potential security risks when utilizing AI tools are relatively straightforward.

• **Establish an AI Usage Policy**
It is critical to set limits and guidelines for AI use prior to installing any AI tools. Be sure to define approved AI tools and vendors, acceptable use cases prohibited data types and data retention practices.

• **Choose Enterprise-Grade AI Platforms**
One way to secure AI platforms is by ensuring that they offer the following: GDPR, HIPAA, or SOC 2 compliant, data residency controls, do not use customer data for training and provide encryption for data at rest and in transit.

• **Segment Sensitive Data Access**
Adopting role-based access controls (RBAC) provides better restrictions on data access. It allows AI tools access to only specific types of information.

• **Monitor AI Usage**
It is essential to monitor AI usage across the organization to understand what and how information is being accessed and including which users are accessing which tools, what data is being sent or processed, and alerts for unusual or risky behavior.

• **AI for Cybersecurity**
One of the primary uses of AI tools is the detection of cyber threats. Organizations use AI to detect threats, deter email phishing, protect endpoints, and automate responses.

• **Train Employees About Responsible Use**
An unfortunate truth about humans is that they are the weakest link in the chain of cyber defense. Even the strongest defensive stance on cyber threats can be undone with a single click by a single user.

AI boosts productivity, but productivity without proper protection is a risk you can't afford. Contact us today for expert guidance, practical toolkits, and resources to help you harness AI safely and effectively.

NAVIGATING CLOUD COMPLIANCE: ESSENTIAL REGULATIONS IN THE DIGITAL AGE

Cloud solutions are the technology darlings of today's digital landscape. They offer a perfect marriage of innovative technology and organizational needs. However, it also raises significant compliance concerns for organizations.

Compliance involves a complex combination of legal and technical requirements. Organizations that fail to meet these standards can face significant fines and increased regulatory scrutiny. With data privacy mandates such as HIPAA and PCI DSS in effect, businesses must carefully navigate an increasingly intricate compliance landscape.

Compliance Regulations

Compliance varies from country to country. It is important to know where data resides and through which countries it passes to remain compliant.

- **General Data Protection Regulation (GDPR) – EU.** Globally speaking, GDPR is one of the most comprehensive privacy laws. It applies to any organization processing EU citizens' personal data, regardless of where the company is physically doing business.
- **Health Insurance Portability and Accountability Act (HIPAA) – US.** HIPAA protects sensitive patient data in the United States. Cloudbased systems storing or transmitting this sensitive information (ePHI) have to abide by HIPAA standards.
- **Payment Card Industry Data Security Standard (PCI DSS).** Organizations that process, store, or transmit credit card information must abide by a set of compliance regulations.
- **Federal Risk and Authorization Management Program (FedRAMP) – US.** Providing a standardized set of protocols for federal agencies operating on cloud-based systems, providers are required to complete a rigorous assessment process.
- **ISO/IEC 27001.** This is an international standard for Information Security Management Systems (ISMS). It is widely recognized as the benchmark for cloud compliance.

Maintaining Compliance

It is vital that organizations realize that cloud compliance is not merely checking items off a list. It requires thoughtful consideration and a great deal of planning. The following are considered best practices:

- **Audits:** Shortcomings are easily recognized and addressed to keep your infrastructure in compliance.
- **Robust Access Controls:** Using the principle of least privilege (PoLP) and MFA
- **Data Encryption:** Whether at rest or in transit, all data must use TLS and AES-256 protocols.
- **Comprehensive Monitoring:** Audit logs and real-time monitoring provide alerts to aid in compliance adherence.
- **Ensure Data Residency:** Ensure that your data center complies with any associated laws for the region.
- **Train Employees:** Providing proper training can help users adopt use policies help protect your digital assets and remain compliant.

HOW THE NEWEST BLACK FRIDAY TECH GADGETS CAN BOOST YOUR BUSINESS

Images of Black Friday no longer merely conjure up visions of bargain-hunting shoppers bullrushing storefronts to secure the best deals. It is now viewed by many organizations as a strategic opportunity to minimize the cost of upgrading their technology infrastructure.

Traditionally, Black Friday tech deals surrounded gaming platforms and entertainment technology, but that has changed. Now, businesses recognize that there are numerous deals on the latest technology that offer real-world value to improve collaboration and productivity.

Best Practices When Buying Consumer Tech for Business Use

A quick look at online tech outlets shows just how steep the discounts can be on Black Friday. While these sales offer great savings, businesses need to approach purchases mindfully. Buying equipment solely because it's discounted defeats the purpose if it cannot integrate into your existing tech environment.

- **Business-Grade Warranty:** Unfortunately, consumer products don't offer the same commercial warranties or support. It is always a good idea to check this for any purchases organizations are considering.
- **Compatibility Assurance:** The new purchases have to be compatible with existing software, hardware, and networks, or it is a wasted effort.
- **Lifecycle Management:** The discounted items need to be tracked and included in the IT management plan to determine when and how the devices will be replaced in the coming years.
- **Secure Everything:** Much like the warranty, not all consumer products come with the same safeguards necessary for enterprise-level security.

Whether you're an MSP or a small business owner, we can help you turn Black Friday deals into year-round results. Contact us today for expert advice.

ADVANCED PROTECTION FOR YOUR LOGINS

Here are several advanced methods for securing business logins:

1. **Multi-Factor Authentication (MFA)**
MFA requires users to provide two verification points.

2. **Passwordless Authentication**
Some emerging frameworks have abandoned the username and password authentication method entirely.

3. **Privileged Access Management (PAM)**
PAM solutions offer secure monitoring and the enforcement of 'just-in-time' access and credential vaulting.

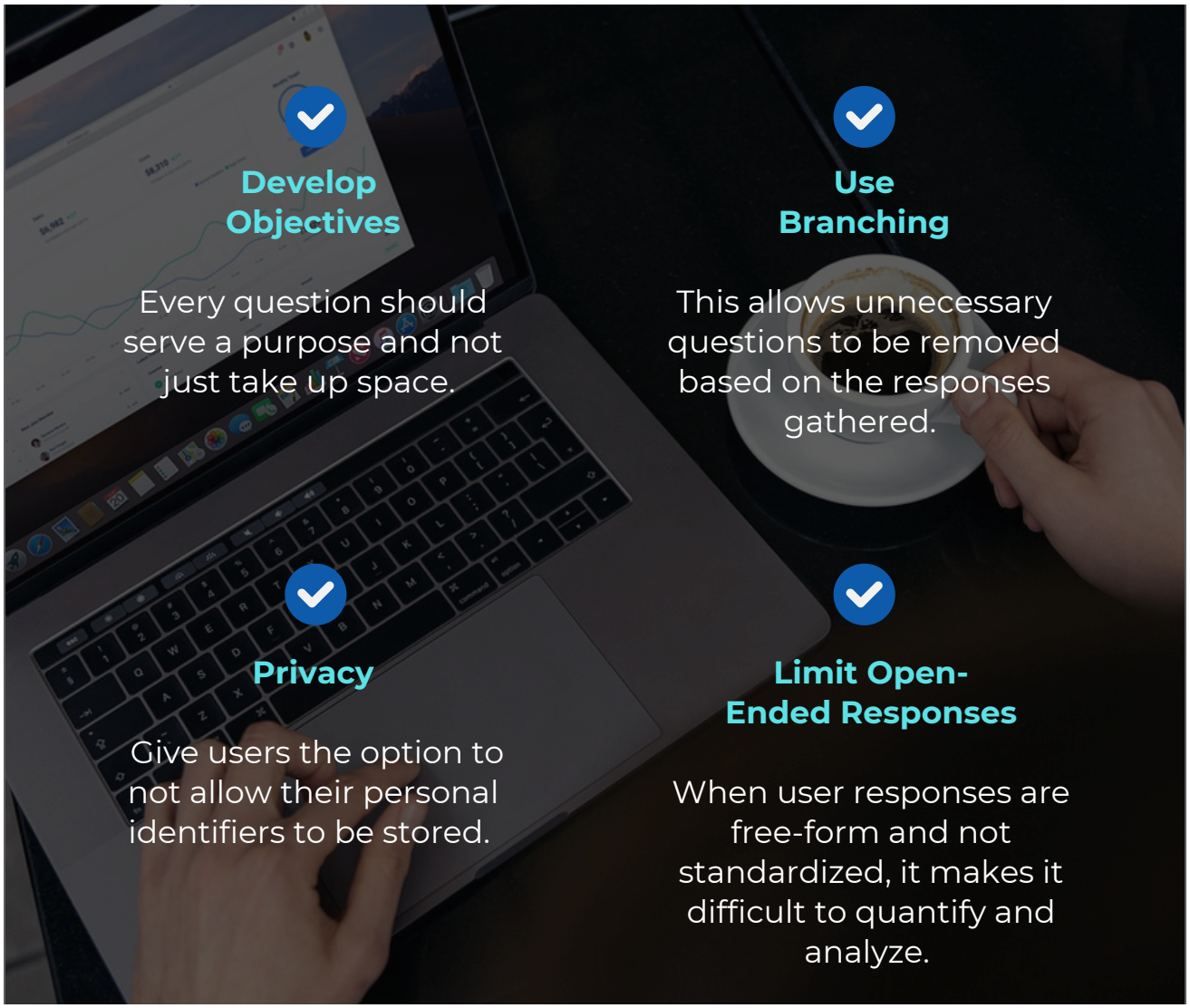
4. **Behavioral Analytics and Anomaly Detection:**
Modern authentication systems employ AI-driven methods to detect unusual behavior in login attempts.

5. **Zero Trust Architecture:**
This architecture adopts the simple principle of "never trust, always verify."

MICROSOFT FORMS TIPS

With its robust feature set and seamless integration into the Microsoft 365 ecosystem, Microsoft Forms provides a secure and compliant platform for collecting and analyzing data.

The best way to get the most out of Forms is to follow a few simple tips:



With the right guidance, resources, and training, businesses can fully harness Forms to transform raw data into actionable strategies, driving smarter decisions and long-term growth.

CREATING AN IT ROADMAP FOR SMALL BUSINESS GROWTH

The IT roadmap is an outline for how technology will drive business objectives. It must always have the following:

- **Assessment:** Create an assessment of all IT assets to have a good starting point.
- **Business Objectives:** Identify the company's top goals over the next 1–3 years.
- **Technology Timelines:** Provide detailed schedules to ensure seamless integration.
- **Budget Forecast:** Calculate to eliminate hidden costs and surprise overages.

A well-maintained roadmap ensures organizational goals remain in focus as IT expansion continues. Here are tips to maintaining it:

- **Collaborate:** The document should reflect company-wide needs.
- **Able to Adapt:** As new technology becomes available, organizations need to update their roadmaps.
- **Partner With Experts:** Consider leveraging external experts for guidance and training opportunities. A phased approach remains the most effective way to achieve lasting impact and steady progress toward your organizational goals.

Thank You!

Thanks for taking the time to read this month's newsletter. We hope you picked up a few helpful tips or ideas to make your tech work a little smarter for you.

If you ever have questions, or just want a second opinion on anything IT-related, we're only a phone call or email away.

CONTACT US BELOW

OASIS TECHNOLOGIES

405.948.6500

info@oasis.tech

oasis.tech

6317 NW 23rd St
Bethany, OK 73008