Outsource Cyber Security for a Safe 2023

Moving into 2023, we face a storm of cyber security challenges, from state-sponsored cyber warfare to the risks inherent in cloud computing. Executives recognize the need for sophisticated defenses, but many organizations lack the necessary skills in-house. When small and mid-sized businesses outsource cyber security, they benefit from enterprise-grade solutions to complex problems.

Outsourcing can play out in a variety of ways. Some organizations will contract with a third party to handle all their security operations. More commonly, a business will hire out certain security tasks while keeping others in-house.

For instance, a cyber security provider may provide network monitoring, freeing up internal security staff to focus on strategic tasks. Or a provider may bring important expertise to penetration testing and security education. Outsourcing can deliver significant benefits when organizations carefully vet their providers and follow outsourcing best practices.

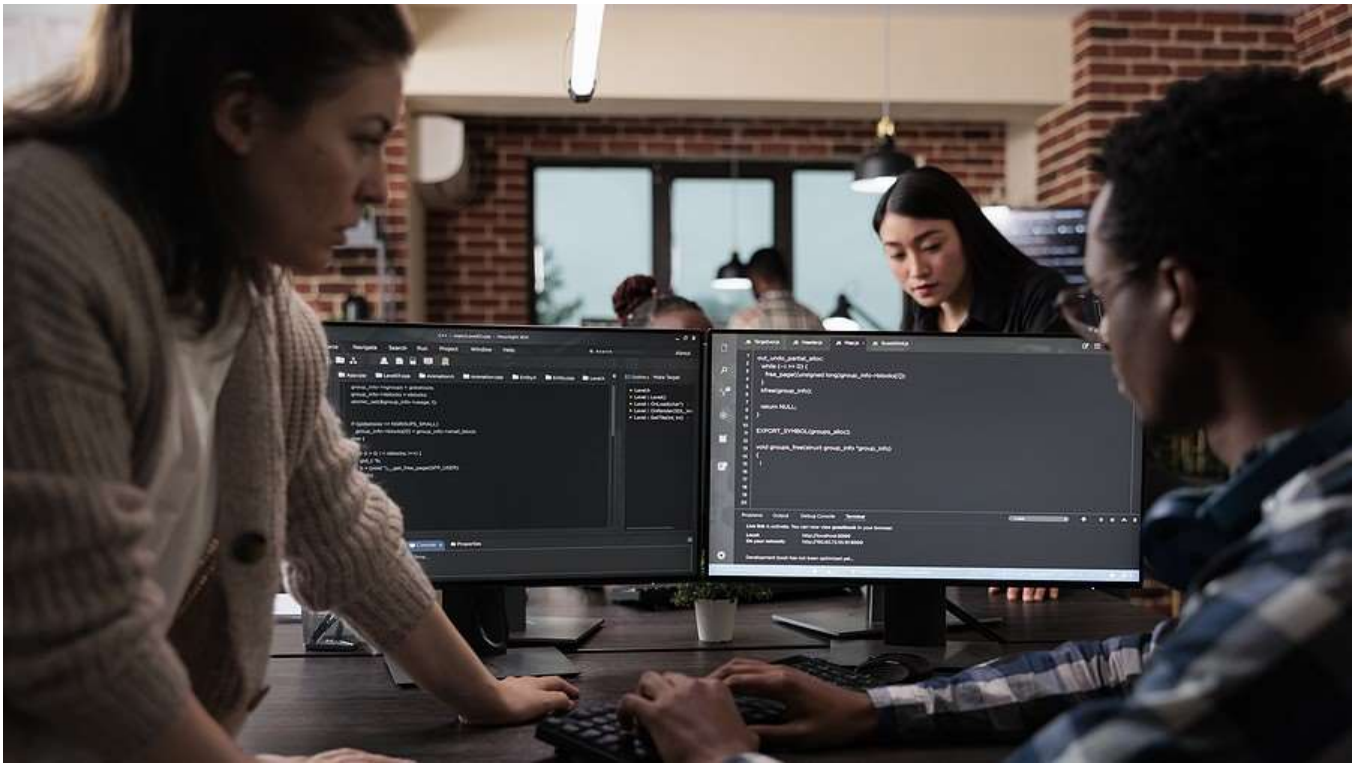
Benefits of Managed Cyber Security Services

Businesses outsource cyber security for several key reasons. In the first place, organizations across the globe struggle to hire cyber security professionals as the cyber skills gap widens. Security providers help to close that gap by delivering the expertise and tools that organizations need but cannot provide internally.

Secondly, by outsourcing, organizations can gain access to 24/7 system monitoring, often using machine learning to proactively address issues. Providers can monitor both on-premises and cloud environments for security and compliance issues. And by combining automated monitoring with human expert analysis, organizations gain in-depth protection.

In addition to 24/7 system monitoring, outside experts deliver risk assessments and penetration testing to identify weaknesses. These assessments form a critical part of informing ongoing cyber security strategy.

Additional key benefits include targeted, professional security awareness training, as well as potential cost savings, scalability and business continuity. And with security experts on tap, the organization can focus on its core business.



Critical Questions to Ask a Potential Cyber Security Provider

When organizations look to outsource cyber security, they should consider the risks as well as the benefits. For instance, not all security providers deliver the same response time guarantees. And some providers may push more technology when they should instead focus on matching technology solutions to business needs.

Consequently, organizations should vet potential security providers carefully. Ask questions such as the following:

- **How will support be delivered?** Most provider will offer multiple support packages. Before signing a contract, know what the contract includes and what it does not include. Services should include 24/7 monitoring and support. Know the support process, including charges for on-site technicians when needed.

- **What does the contract cover?** In addition to monitoring, does it include services such as security testing, backups, cloud-based SIEM and email protection? Expect specific, detailed answers. Make sure you can scale services up or down as needs change.
- **What is the guaranteed response time?** Response time typically varies depending on the support level purchased and the severity of the issue. A critical issue may generate a 15-minute response time, versus an hour or two for a medium priority issue.
- **How much do these services cost?** Most providers will charge a flat monthly fee that varies depending on the desired level of support. Know what your monthly fee buys you and how much additional services cost.
- **Does the provider have the expertise you need?** Security providers may specialize in different industries and various services. Make sure you contract with a provider that knows your industry and the specific challenges you face. And ensure that they provide services that meet security needs you have previously identified.
- **References.** Always ask for references and take the time to talk with customers who have experience with the provider you are considering.

Tips for Success When You Outsource Cyber Security

Outsourcing cyber security involves a partnership. And like all successful partnerships, it requires good communication. Each side should clarify expectations up front. For instance, know the time and effort your in-house staff will need to commit. Be clear about necessary processes, as well as regulatory requirements.

To drive communication, schedule regular meetings with your cyber security provider. This will keep you informed about security updates and allow you to communicate any strategic changes.

Tap into the expertise you pay for. A quality managed services provider can help you evaluate current processes and choose the right strategies and technology to adopt moving forward. Explore additional solutions the provider can offer to round out your cyber security approach. For instance, your service provider can play an essential role in your disaster recovery plan.

Consider an experienced cyber security provider such as eMazzanti. Whether you need specialized security services or a comprehensive cyber security solution, we have the tools and expertise to keep your business safe in 2023.