NEW CYBER SOURCE

Fully Managed Security Services: Because Security Should Never Be Left to Chance

☑ *Today's most savvy, security-conscious organizations have accepted the realities of cybercrime and are curtailing their defensive "maneuvering." While a strong security defense will always be important, it must be paired with robust employee training, swift detection and decisive incident response and remediation. New Cyber Source's targeted security package checks every box.*

With reported data breaches hitting an all-time high every successive year, and 92 percent of breaches going undetected by the targeted organizations, cybersecurity must be at the forefront of every organization's awareness. Yet, many companies still have no reliable mechanism for discovering—or mitigating the damage from—these attacks.

Making matters worse, more than three-quarters of intrusion are not detected by internal security processes. Rather, they are discovered by outside entities—law enforcement, vendors, partners and others. To ensure business continuity in the face of this onslaught, business leaders must focus their efforts on specific points of intelligence:

- Defensive tools cannot prevent breaches: Even the best security software cannot close every possible "tunnel" to the heart of your data. The best-protected firms also focus on incident response and mitigation.
- Mistakes are a leading cause of breaches. Thanks to the ever-present "people factor," no firm is immune from a breach. In fact, human error—lost devices, credential theft, poor email practices, and more—accounts for half of all data breaches.
- Security is a practice, not a procedure. To have the greatest possible odds of minimizing theft or compromise of assets, damage to corporate reputation, loss of client trust, and possible criminal liability, firms must develop and maintain a comprehensive security practice that begins with hard-nosed assessment and "hole closure," and incorporates ongoing personnel training and threat mitigation paired with rapid post-attack incident response and mitigation.

> *Every year, reported data breaches hit a new high, yet 92 percent go undetected—until an outside entity discovers them.*

We offer a wide range of expertise:

Architecture & Capacity Planning
Asset Discovery & Management
Cloud Security
Data Backup & Recovery
Disaster Recovery
& First Responder
Hyper Converged Infrastructure
Managed IT Services
Managed Security Services
Penetration Testing
Risk Management & Governance
Security Assessments
SIEM/Log Management &
Threat Protection
Specialist Practices
Training

We serve a wide range of industries:

Energy & Power
Financial Services
Healthcare
Hospitality
Information Technology
Manufacturing
Pharmaceutical
State & Local Government
Telecommunications
Utilities

We offer a wide range of expertise:

Architecture & Capacity Planning
Asset Discovery & Management
Cloud Security
Data Backup & Recovery
Disaster Recovery
& First Responder
Hyper Converged Infrastructure
Managed IT Services
Managed Security Services
Penetration Testing
Risk Management & Governance
Security Assessments
SIEM/Log Management &
Threat Protection
Specialist Practices
Training

We serve a wide range of industries:

Energy & Power
Financial Services
Healthcare
Hospitality
Information Technology
Manufacturing
Pharmaceutical
State & Local Government
Telecommunications
Utilities

Shield Your Firm Against the Inevitable

At New Cyber Source, we deal in realities. We don't paint rosy pictures of breach-free landscapes, because we don't promise the impossible. The hard truth is that if you haven't been breached yet, you will be.

As battle-hardened technology warriors with decades of experience among our staff, we use a tested, proven methodology to equip you with weapons that minimize your risk of intrusion, and dramatically reduce your risk of exposure and loss due to a security incident.

Security Risk Assessment

Pairing advanced technologies such as penetration testing with empirical evaluation of company policies, employee behaviors, and more, our security experts identify where you are exposed and develop a plan to close each potential attack point. If we find that you have already been breached (which isn't uncommon), we will go into hyperdrive to close any holes and mitigate the damage.

Active Threat Intelligence

Our seasoned software team deploys and configures industry-leading threat intelligence technology, which continually investigates Internet traffic to identify IP addresses with sinister characteristics, score them based on level of concern, and mark them as either blocked or safe and allowed network access.

Simplified, Secure Password Control

We protect your system, device and user passwords with a leading privileged access and identity management tool. All passwords are stored securely with military-grade, 256-bit AES encryption, and accessing or changing them requires multi-factor identification.

During daily operation, no passwords are needed, because each system or app access request by an authorized individual generates a time-based, one-time passcode (TOTP) that can be used or shared with vendors; contractors and other off-network users without exposing the underlying password.

Advanced Email Security

Unlike many firms, we don't install an email filtering program and walk away. We deploy a security technology called content disarm and reconstruction, which scans incoming emails and removes all elements that fail a stringent malware analysis.

This approach is proven effective against the zero-day vulnerabilities that wreak havoc in even well-secured organizations. In addition, we train your personnel not to make the foolish mistakes that are a prime source of infection and breaches.

Intrusion/Advanced Persistent Threat Detection

Our teams deploy multiple agents to continually scan the network for the signatures of possible threats to detect and eliminate them. If one should slip past us, we sandbox it immediately, so any damage is extremely minor.

Penetration Testing

In addition to our initial penetration testing, we perform ongoing "test attacks" to ensure your network and systems are still maintaining appropriate defenses and cannot be penetrated. If we find any weaknesses, we close them immediately.

Asset Mapping

Our digital forensics specialists audit and map your technology assets to ensure there are no rogue devices on the network—and to confirm the ones there, are properly configured and responsive. Audits like these not only help secure your environments; they also provide support for compliance efforts.

Governance, Risk Management and Compliance (GRC) Consolidation

Our governance experts examine and optimize your technology GRC plans and programs, which both helps ensure regulatory compliance and maximizes operating efficiency.

End Point Security

Because the corporate attack surface is so broad, we move beyond network security to securing every corporate endpoint with which it interacts. Using industry-leading protection and remediation technologies, our tools break the attack chain through multi-vector (static and dynamic) malware detection—with automated remediation if a bug temporarily escapes our net—plus malicious website blocking, ransomware blocking and exploit protection.

Technical Staff Training

Our training experts ensure your technical staff is fully trained and up to speed on traditional, current and evolving security procedures and techniques—and that they know precisely what to do in the event of an intrusion. (For those companies that do not have in-house technical staff, we can even help you hire the best and brightest—and then train them, too.)

GDPR Readiness

With the General Data Protection Regulation (GDPR) effective as of May 2018, firms can no longer ignore this mandate. New Cyber Source has studied the GDPR in detail and developed an extensive test that ensures firms comply with GDPR – and can avoid the massive ($20M+) fines that can result from a violation.

Post-Incident Forensics

After a threat has been defused and the incident response is complete, our team will scour activity logs and other digital traces to find out exactly how the incident occurred. Armed with that information, we can make proactive recommendations for making the organization's security posture even more robust.

Prepare for and Respond to a Digital Assault

Our security mechanisms are designed to prevent an intrusion, but the reality is that no currently available combination of technologies can 100% guarantee any firm will not be breached. (Hire us, and if that situation changes, you will be the first to know.) To address this challenge, we have developed an end-to-end program to ensure firms are ready for an incident and can respond in the most timely and effective manner possible.

Incident Response Readiness Review

New Cyber Source's heavily trained and certified incident response experts will assess your current response plan and make recommendations for improvements. Elements of the effort include:

- Evaluate security monitoring and response capabilities.
- Explore current procedures and benchmark them against incident response best practices.
- Assess current response plan against the latest threats and the mechanisms identified to help mitigate them.
- Deliver our findings with a roadmap of recommendations prioritized by which investments will have the greatest impact upon your security posture—and yield the most ROI.

First Responder Security Incident Response

Our computer security incident response experts become your on-call front line of defense, ready to address incidents quickly and effectively as they occur. During the most stressful period any organization will face, our Incident Response Retainer (IRR) reduces the mean-time-to-containment and the mean-time-to-remediation. With a retainer in place, we are ready to assist when you need us most.

New Cyber Source Guarantees

- 24/7 availability to Incident Responder (IR) experts
- Initial contact established within 3-hours
- Actively working the incident within 24-hours
- Ability to convert unused hours to consulting services
- SLA backed by money-back guarantee

Turning Your Data Stores Into Fort Knox

In conjunction with our security services, we recommend clients allow us to evaluate the security of their data storage locations.If appropriate, we will make recommendations for transitioning to hyper-secure cloud storage, managing it proactively (Storage as a Service; Data Center as a Service) to optimize security. Our cloud storage recommendations have been prescreened for their adherence to the most advanced security protocols. Transitioning to these providers reduces staff burden and eliminates the headaches of developing and managing truly secure storage with limited staff—or expensive contractors.

Be Safe…not Sorry

It is impossible to overstate the extreme risk faced by inadequately protected organizations. As soon as companies close one type of vulnerability, hackers find another one. Recently, they have been targeting improperly configured cloud environments. New Cyber Source stays abreast of these developments and can act upon them much faster than the vast majority of in-house security teams—and we run circles around most security providers.

In short, New Cyber Source gives you the best possible chance of avoiding a breach—and of minimizing repercussions if one occurs.

Furthermore, both government agencies and victims have tired of excuses and are pursuing legal and civil action against firms that experience major breaches—and even those who have merely exposed themselves to the possibility of one. From the smallest business to a Fortune 100 corporation or a public sector entity, no one is excused.

If you think we are being alarmist, consider this: An American power company will be paying an unprecedented $2.7 million penalty over security oversights that could have allowed hackers to gain remote access to the power provider's systems. Power regulators reached the settlement after a security researcher found that more than 30,000 company records were unprotected online. We'll never know if hackers might have found them, or not. The power company and its stockholders still paid the price.

Phone: 404.641.6724
Email: info@newcybersource.com

NEW CYBER SOURCE
925 Sanders Road Cumming, GA 30041
www.newcybersource.com