Cybersecurity Solutions and Services Suite

With one touch, a threat can become a reality.

Empowering people who serve the public®

tyler technologies

Shedding light on cybersecurity readiness and resilience

The cost of cyberattacks puts everyone at risk.

The world is witnessing a paradigm shift in information delivery, logistics, and lifestyle. Digitization of data has become the foundation of our global infrastructure, opening a floodgate for cyberthreats.

When mitigating the impact of a cybersecurity breach, how you plan and how you react is the difference between being secure and being vulnerable. The question is not if, but when an attack will happen. Cybercriminals do not discriminate. Private, local, state, and federal organizations are all a target.

Tyler Cybersecurity's 24/7 Managed Detection and Response, Risk Assessment/Mitigation, Planning, and Policy Development solutions monitor, prepare for, and fortify networks and valuable assets against external and internal cyberattacks – integrating accelerated response tactics and solutions.

The Cybersecurity Lifecycle

Preparing today for a more secure tomorrow.

Achieving cybersecurity resilience is a holistic, ongoing effort made up of three core fundamental elements: detection, strategy, and testing. Factoring each element into the cybersecurity process ensures organizational effectiveness against a dynamic and evolving threat environment — the cybersecurity lifecycle.

Your partner in strengthening network security

The external threat environment is ever evolving.

Cybercriminals are continuously seeking and creating avenues to infiltrate networks and wreak havoc on organizational stability and performance. If breached, the response to detect, isolate, and eliminate the threat must be a conscious, planned effort to ensure the preservation of your networks and valuable assets.

Cyberattacks, it's not if... but when an attack will occur.

How vulnerable is your organization to a threat? How you respond to safeguarding your network, valuable assets, and reputation is the difference between a ready response and being victimized by a potentially debilitating outcome. Tyler Cybersecurity's suite of services and solutions span cybersecurity readiness, strategic planning, training, and testing with real-time 24/7 threat detection.

We develop more than cybersecurity solutions. We establish trust, confidence, and peace of mind. Our team of specialists are innovators in the field of cybersecurity, recognized for developing leading edge cybersecurity solutions and services — bridging the gap between technology and human interaction.

Cybersecurity spending to exceed $1.75 trillion by 2025

Cybercrime damage to hit $10.5 trillion annually by 2025

Ransomware costs to reach $265 billion by 2031

Cybersecurity Solutions

Evaluate, Plan, Test and Detect ... Cybersecurity Resilience and Readiness

Advisory: Governance, Strategy, and Guidance

Given the complexity of today's evolving cyberthreat landscape, Tyler Cybersecurity's comprehensive advisory services are designed to provide expert insight, guidance, and council when navigating cybersecurity effectiveness and volatility. From policy and procedure development encompassing risk, incident, and third-party management, to employee education and training, regulatory and audit compliance, disaster recovery and business continuity planning, Tyler Cybersecurity's advisory team of certified professionals assists organizations with planning for and responding to today's most advanced cyberthreats.

Policies, Procedures, and Planning

Working in direct collaboration with your team, our cybersecurity professionals assess current security practices and guides your organization to build upon them with comprehensive strategies and processes tailored to your specific business objectives and goals.

Education and Training

Employees are your first line of defense against a cyberattack and can also be your weakest link. Tyler Cybersecurity develops tailored training sessions designed to cultivate a critical-role-culture in protecting your organization and valuable assets.

Risk and Compliance Management

Assessing and managing risk requires a practiced methodology to drive informed decision-making. Our team assists you with assessing, prioritizing, and managing your organization's security risk - enhancing the security readiness of your organization.

Network Testing and Assurance

Critical to cybersecurity readiness and resilience, Tyler Cybersecurity's network testing services uncovers critical vulnerabilities to establish overall global system effectiveness and readiness. Tyler Cybersecurity's team of testing experts identify and expose vulnerabilities by conducting penetration tests, social engineering, phishing, and vulnerability assessments specific to your network, identifying issues before a threat becomes a breach.

Vulnerability Assessment

Routine scanning of your network allows you to identify known vulnerabilities and levels of severity to proactively prioritize and remediate. Tyler offers remote scanning and delivers easy to navigate report functionality with remediation recommendations.

Penetration Testing

Identifying network susceptibility to the exploits of hackers is essential in mitigating cyber risks. Our team of cybersecurity experts attempt network access and provide you with outcome-based findings to prioritize mitigation and remediation efforts.

Social Engineering

Employees are the epicenter of security controls. It's crucial to ensure organizational training establishes a cyber-aware culture. Our social engineering phishing assessment identifies weaknesses that could enable attackers to target staff and infiltrate your network.

Rapid Threat Detection and Response

Tyler Cybersecurity's 24/7 Managed Detection and Response solution analyzes, detects, and informs organizations of viable cyberthreats spanning internal and external networks to perimeter endpoints. Supported by Tyler Technologies internal Security Operation Center (TSOC), comprised of cybersecurity analysts and powered by artificial intelligence and machine learning, Managed Detection and Response identifies threats with unrivaled speed and accuracy to avoid the catastrophic impact of a network breach.

Real-Time Alerts

If actively at risk, Tyler Cybersecurity Analysts contact you immediately.

- Customized, automated alerts for administrative changes, Microsoft 365, Active Directory, and more
- Identify and confirm unique and suspicious activity
- Detailed occurrence notifications sent immediately
- Request authorization capability to disable infected Windows machines to mitigate suspicious activity

Reporting

Cybersecurity analysts prepare daily network traffic summaries specific to your organization.

- 24-hour critical log data reports
- Receive monthly report summaries
- Monthly threat and findings management reports and summaries
- Secure and documented audit trail for compliance

Secure Online Portal

Gain insight into all your network traffic online 24/7 with Managed Detection and Response's secure online portal.

- Search and filter your report data with customizable, ad-hoc reporting capabilities
- Access interactive dashboards to quickly review, and respond to findings
- Access and review SOC threat intelligence

Identifying threats before they become a breach.

Cybersecurity touches every aspect of an organization

Your technology stack is only part of the strategy.

Aligning cybersecurity operations with organizational business goals to include people, process, and planning plays a crucial role in maintaining and improving cybersecurity posture, culture, and workflows. Taking a methodical approach to progressing through the levels strengthens cybersecurity defenses to mitigate risk exposures and expand program performance.

Levels of cybersecurity program progression

People

Sustained	Integrated cybersecurity culture supported for continuous improvement
Replicate	Defined responsibilities, assigned roles, and heightened awareness
Managed	Defined responsibilities and roles with improved awareness
Aware	Established leadership and limited awareness
Basic	Minimal staff and awareness

Process

Sustained	Documented program tracked and updated for continuous improvement
Replicate	Defined program with formalized processes tracked across the organization
Managed	Basic program in place with organization-wide processes and policies
Aware	Established basic processes and policies
Basic	No formal cybersecurity plan

Technology

Sustained	Comprehensive controls in place and reviewed for continuous improvement
Replicate	Controls fully implemented, monitored and tracked
Managed	Managed controls documented with better oversight and coordination
Aware	Basic controls, oversight, and documentation
Basic	Limited controls and oversight

Because not every organization is the same

Packaged cybersecurity solutions and services.

Implementing structure into your cybersecurity discipline at an expanding scope can be a daunting task. Tyler Cybersecurity's suite of subscription-based solution services provide a strategic, purpose-driven path forward in support of your strategic business, operational, and security objectives across all stages of the cybersecurity lifescycle.

Cybersecurity Awareness

- Managed Detection and Response (two week service solution install)
- Acceptable use policy with data handling matrix
- End user cyber awareness / phishing training
- Email phishing campaign
- One day follow-up end user training
- Annual leadership meeting

Ransomware and Audit Readiness

- Managed Detection and Response (two-week service solution install)
- External penetration test with vulnerability scan
- Internal vulnerability scan
- Incident response plan creation/update
- Incident response plan tabletop exercise
- Acceptable use policy with data handling matrix
- Information security policy set creation and update
- Cybersecurity training
- Annual leadership meeting
- Quarterly advisor call

Comprehensive Preparedness

- Managed Detection and Response (two-week service solution install)
- External penetration test with vulnerability scan
- Internal configuration and vulnerability assessment (CAVA)
- Acceptable use policy with data handling matrix
- Information security policy set creation and update
- Incident response plan creation/update
- Incident response plan tabletop exercise
- Business impact analysis
- IT risk assessment
- Cybersecurity training
- Email phishing campaign
- Annual leadership meetings/training
- Monthly advisor call

We protect organizations with cybersecurity solutions and services.

We analyze and detect threats ... with precision.

We test and identify vulnerabilities ... with purpose.

We strategize, plan, and advise ... with results.

We transform the every day ... for a better tomorrow.

Tyler Technologies (NYSE: TYL) provides integrated software and technology services to the public sector. Tyler's end-to-end solutions empower local, state, and federal government entities to operate more efficiently and connect more transparently with their constituents and with each other. By connecting data and processes across disparate systems, Tyler's solutions are transforming how clients gain actionable insights that solve problems in their communities. Tyler has more than 37,000 successful installations across more than 12,000 locations, with clients in all 50 states, Canada, the Caribbean, Australia, and other international locations. Tyler has been recognized numerous times for growth and innovation, including Government Technology's GovTech 100 list and Forbes' "Most Innovative Growth Companies" list. More information about Tyler Technologies, an S&P 500 company headquartered in Plano, Texas, can be found at **tylertech.com.**

800.772.2260 | info@tylertech.com | tylertech.com

TO-CYB-ASB-22284-1221

tyler technologies

Empowering people who serve the public®