

Cybersecurity: Threat and Response

The nation's vital interests are intertwined with IT infrastructure. Security must now be built into systems, networks, and applications from the start.

An Executive Briefing

from



Telos Corporation
19886 Ashburn Road
Ashburn, VA 20147-2358

Toll Free: 1-800-444-9628
Website: www.telos.com
Twitter: @telosnews
Facebook: facebook.com/teloscorporation

Cybersecurity: Threat and Response

The nation's vital interests are intertwined with IT infrastructure. Security must now be built into systems, networks, and applications from the start.

High-profile IT security incidents are casting a spotlight on cybersecurity and the critical role it plays in national defense, homeland security, and commercial activity. These incidents are in turn compelling government agencies, defense and federal contractors, and technology vendors to ensure the integrity of the systems they use and purvey.

Key civilian agencies, the DoD, and the intelligence community are advancing standards and best practices for IT security that can be shared across the federal domain. These standards also extend to their contractors, who participate in “virtual enterprises” that must be just as strongly protected in today’s Web-enabled business environments.

IT companies are finally acknowledging that a technology solution without security inherent in its design and development is no solution at all.

In response, mainline technology companies have acquired IT security vendors to retrofit security into their offerings: Intel has purchased McAfee, HP acquired Fortify and ArcSight, Dell acquired SecureWorks, and IBM acquired BigFix and Open Pages. These transactions show that IT companies are finally acknowledging that a technology solution without security inherent in its design and development is no solution at all.

That position has been the driving philosophy behind Telos Corporation for more than a decade. Telos offers a diverse range of enterprise solutions, each of which shares the company’s deep heritage in IT security and information assurance with security built into them from the start.

This paper is intended to outline the capabilities of Telos Corporation as a provider of leading-edge solutions for communications, systems, networks, and access that feature cybersecurity designed into them as a matter of course. It begins with a summary of the threat situation and the responses of federal agencies and the Department of Defense. It concludes with an overview of Telos’ comprehensive approach to improving the security postures of our customers through complementary offerings that provide critical pieces of the cybersecurity puzzle.

The Cyber Threat – From Careless Insiders to State Sponsored Malicious Activities

The cybersecurity threat is multi-dimensional and the technology used to compromise the country’s systems is growing in volume and sophistication. Targets include not only military and federal systems in the U.S. but also private sector infrastructures that play a

prominent role in the country's economic life. Several recent compromises demonstrate the emergence of new actors and highlight where vulnerabilities remain:

- In December 2009, hackers believed to be working for North Korea stole a classified file of U.S. war plans for the Korean peninsula from an unprotected USB drive inadvertently left on a computer exposed to the Internet – a clear failure to follow procedures to protect sensitive information and to encrypt data at rest.
- In that same timeframe it was also widely reported that Iraqi insurgents could intercept Predator video feeds using relatively unsophisticated software available over the Internet. Here there was a failure to protect communication networks carrying sensitive information.
- In August 2010 it was revealed that a major breach of U.S. defense networks that occurred in 2008 was the result of a single USB drive containing malicious code being inserted into a laptop at an American base in the Middle East. The malware was placed on the drive by a foreign intelligence agency; from there, it was uploaded to a Central Command network.
- The Chinese government and its People's Liberation Army have for several years staged or sponsored high-profile cyber attacks or intrusion attempts against American corporations (including defense contractors), the Department of Defense, federal agencies, and at least one member of the U.S. Congress. Their incursions have also come against allied governments, global enterprises, and human rights activities in their own country.
- Cyber attacks that target the intellectual property of U.S. businesses is another emerging threat that could have severe economic impacts – estimates of intellectual property data thefts ranged up to \$1 trillion for 2008, according to security firm McAfee.

Government Response – A Focused Effort to Develop a Capable and Nimble Cybersecurity Infrastructure

Recognition of our dependence on information technology and its increasing vulnerability to emerging threats have spurred the federal government to effectively coordinate its response and increase the resources dedicated to enhancing our cybersecurity.

Increasing vulnerability to IT threats has spurred the federal government to increase the resources dedicated to cybersecurity.

The current and previous administrations have reviewed cybersecurity policy and provided a number of short- and mid-term goals for setting the agenda for the federal government and creating high-level organizational structures to ensure that cybersecurity receives presidential attention and a commensurate level of resources. These actions involve many government agencies, but most notably the Department of Homeland Security and the Department of Defense.

On January 2, 2008, President Bush signed National Security Presidential Directive 54/Homeland Security Presidential Directive 23, which established the Comprehensive National Cybersecurity Initiative (CNCI). The CNCI formalizes a series of efforts to further safeguard federal government systems from cyber threats and attacks. While classified, this directive galvanized the government's current efforts and helped frame discussion of government efforts in this area.

Earlier, the Department of Homeland Security had established National Cyber Security Division to serve as its central organization for increased efforts to protect IT infrastructure. NCSA was formed by consolidating a number of existing IT security offices to build and maintain an effective national cyberspace response system and to implement a cyber-risk management program for protecting critical infrastructure.

The Obama administration led an early effort to review the country's cyberspace policies. The president directed a 60-day, comprehensive, "clean-slate" review to assess U.S. policies and structures for cybersecurity. The goals from this review form the agenda for the administration and the new cybersecurity organization in the White House.

After some delay, the president nominated a cybersecurity "czar" within the National Security Council in December 2009. Increasingly, in the face of ever-changing threats, the emphasis is on risk management, mission assurance, agility and resilience, and proactive efforts to both protect our assets and thwart those who would compromise those assets.

Focus on the Department of Defense

The Department of Defense has been an early proponent of strong and deep network defense, both because DoD has been the focus of many of the security incidents and because it has the most to lose in both capability and sensitive information. These efforts have put DoD in a leading position to achieve secure network operations, as well as both information and technology dominance of cyberspace. These initiatives culminated in 2009 with the Department of Defense proposing the formation of a DoD Cyber Command focused on both offensive and defensive aspects of the cyber environment.

DoD defines cyberspace as the global domain within the information environment consisting of the interdependent network of IT infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processes and controllers. Necessarily broad in both its application and implications, cyber protection has been an emerging priority and the focus of development of organizations to improve our defenses.

Even further, it is the basis for a new doctrine to both protect our assets and effectively attack, when directed, the information assets of our enemies. Army Lt. Gen. Keith Alexander, the former Commander Joint Functional Component Command for Network Warfare and the current head of the new Cyber Command, told the Congress, "Maintaining freedom of action in cyberspace in the 21st century is as inherent to U.S. interests as freedom of the seas was in the 19th Century, and access to air and space in the 20th century."

This doctrine was further developed by Defense Deputy Secretary William Lynn III in an article published in the September/October 2010 issue of *Foreign Affairs*. In that article, called “Defending a New Domain,” Lynn gave a brief account of recent cyber incidents and responses by DoD and emphasized the vital role IT plays in the modern military. He also articulated a strategy of “five pillars of cybersecurity” for not only protecting the military’s IT systems and networks, but for establishing the new mindset needed to accomplish this strategy:

- Cyber must be recognized as a warfighting domain equal to land, sea, and air, a de facto state of affairs since the establishment of Cyber Command;
- The military must extend its defensive posture beyond mere good computer hygiene to include operations for rapid response;
- Cyber defenses must go beyond DoD’s domain to encompass commercial networks, as governed by the Department of Homeland Security;
- Cyber defenses must be coordinated with our global allies for a 21st century update to the “shared warning” construct of the Cold War; and
- DoD must do its part to maintain the country’s technological strength and improve its acquisitions process to align with the rapid development of new products and systems by the IT industry.

The new emphasis on cybersecurity will affect operations and processes across all federal agencies, the DoD, and the intelligence community. To comply with this new era, the commercial providers of IT solutions must ensure their offerings have solid security planned and integrated into them from their inception.

An Industry Response: Technology Solutions with Security Built In from the Start.

The essence of increasing the nation’s cybersecurity is increasing our trust in IT systems and networks and in the people who use and manage them. Telos helps its customers reach this level of trust with solutions that include the most critical cybersecurity standards and regulations.

Telos offers IT solutions for secure communications, systems, networks, and access across the enterprise. Our enterprise-level perspective on IT security ensures that the security measures and methodologies used across all of these solution areas are mutually reinforcing; every Telos solution benefits from the best practices and processes used in all Telos solution areas.

Networks

Telos is at the forefront of designing, developing and provisioning secure networks for the federal government – wired and wireless, in both fixed and mobile configurations. The

introduction of military-grade security for wireless networks has revolutionized the way forward deployed units keep in contact with other elements, share information and intelligence, and access support applications. These same secure networks can empower Homeland Security agencies and first responders with applications requiring stringent security, such as border surveillance, port, harbor, and rail security, secure videoconferencing, and communications interoperability among state, local, and federal jurisdictions.

Telos is at the forefront of designing, developing and provisioning secure networks for DoD and the federal government – wired and wireless, in both fixed and mobile configurations.

Telos has deployed the newest wireless technologies in adverse, communications-poor environments that previously required a fixed communications infrastructure and “headquarters.” These rugged, portable wireless networks support even very small forward elements. For example, Telos is delivering the Army’s next generation high-speed, long-range wireless network. CAISI (the Combat Service Support Automated Information System Interface) is a communications system in transportable cases that is being fielded to logistics organizations worldwide. These secure, tactical wireless LAN modules provide last-mile connectivity from warfighters in operational environments to their logistics networks.

Telos also provides network solutions that leverage emerging technologies for command and control, enterprise network management, geomapping, and “green” facilities management. These rapidly developed and deployed applications can give federal agencies, the DoD, and private enterprises capabilities for sharing information and collaborating in real time using smart devices, tablets, and multi-user, multi-touch interfaces.

Access

Building trust in the people who access cyberspace is a key part of cybersecurity. Telos ID delivers with identity assurance and access management solutions for the federal sector, the DoD, and commercial enterprises.

Telos ID provides the hardware and infrastructure to support the largest and most sophisticated employee credential system in the world – the Department of Defense’s RAPIDS system, which credentials over 10 million people from about 4,000 locations around the world with smart-card-based Common Access Cards (CAC) that contain the secure Public Key Infrastructure (PKI) credentials needed for logical access to DoD systems.

Telos ID provides the hardware and infrastructure to support DoD’s RAPIDS, the world’s largest and most sophisticated employee credential system.

Strong identity vetting is another area where Telos provides solutions and services to ensure that the “people” part of cybersecurity remains secure. Telos ID has built a unique lifecycle-based system that can provide customers real-time access to background-checking databases, FBI and State Criminal History Record Information (CHRI), and authorized government databases that provide continuous review and assurance on the human side of cybersecurity. These capabilities underlie the IDVetting background checking services for employees, job candidates, and

contractors to secure work environments, reduce risk and cost, and comply with laws requiring such checks

Telos ID has extended its expertise in identity systems into physical access as well – supporting the Defense Biometric Identification System (DBIDS), which uses real-time authentication of the credential, the option for biometric authentication, and threat-based authentication to authorize access to military facilities around the world. Similar capabilities are at the heart of Telos ID’s Mobile Authentication and Authorization Control (MAAC) system for secure venue access control at stadiums, arenas, and concert halls.

Systems

Much as there is a requirement for continuous surveillance of the people who access networks and facilities, there is an equally important need for surveillance of the applications that operate on networks as well as of the network defenses themselves.

The facet of Telos that meets this cybersecurity need is information assurance. Telos has been a leader in the development of tools and the provision of security analysts responsible for risk management and mitigation for networks and applications on behalf of Telos customers, including federal agencies, the DoD, the Intel Community, and financial institutions.

Telos products and highly skilled security analysts are at work 24x7 protecting some of the most important networks in the world.

Telos was a pioneer in the development of enterprise solutions that automate the leading government and industry processes for assuring information security and integrity. Xacta IA Manager brings an innovative, repeatable and systematic approach to the wide range of government and industry security processes, including DIACAP, DCID, CNSS 1253, NIST, FDCC/SCAP, FISMA reporting, HIPAA, Sarbanes-Oxley, GLBA, COBIT, and ISO 27002, making it both easier to do an effective review and increasing the sophistication and completeness of the review.

Although a review at a point in time is useful and necessary, it is never enough to ensure effective cybersecurity. Telos products and people assist customers in the continuous monitoring and assessment of networks to ensure ongoing, proactive, effective security as well as the detection and remediation of emerging threats to the networks.

Telos products and highly skilled security analysts are at work 24x7 protecting some of the most important networks in the world. In 2009, 360 million probes and cyber attacks were made against Pentagon computers. Telos uses the information learned from these incidents to improve our information assurance knowledge. With this knowledge we can improve the protection services we provide to our customers, as well as improve our tools that provide information assurance assistance.

Communication

In the Department of Defense and the Intelligence Community, even highly secure networks -- constantly reviewed for vulnerabilities and accessed by trusted, credentialed personnel -- are not secure enough. The cyber assets our country relies on most are the DoD’s

command and control systems – and providing clear, reliable and secure information and instructions throughout these systems is critical to our country’s security.

The nexus of all cybersecurity has to be reliable message traffic that ensures three things – secure transmission, utmost confidence in the identity of the command authority that authored the message, and equal assurance that only intended recipients will receive the message. The DoD system for this is the Defense Messaging System (DMS), which has provided good service for many years but did not make the transition to the current digital world.

AMHS supports over 70 organizations around the world, including the Joint Staff and all Combatant Commands.

Bridging the current secure message infrastructure to the digital world is Telos’ Automated Message Handling System (AHMS). AMHS was developed as a part of the next-generation of the DMS, providing a cost-efficient Web-based solution that greatly simplifies configuration management, system administration, and customer interface to the DoD messaging system.

AMHS supports over 70 organizations around the world, including the Joint Staff and all Combatant Commands, and has been selected as the enterprise messaging solution for all services in the DoD. Accredited to meet DCID 6/3 for Protection Level 3 (DCID 6/3 PL3), AMHS is also used by the intelligence community. AMHS is also in use by civilian agencies that require the highest levels of messaging assurance, such as DHS, DEA, and FAA.



Four aspects of cybersecurity, four solution areas that provide a comprehensive, multi-disciplinary approach to cybersecurity. Telos’ value proposition for cybersecurity is a powerful one: cutting-edge offerings for differing aspects of enterprise IT requirements, all with cybersecurity built in from the moment of conception.

Telos secure solutions have been deployed in support of the most demanding and significant customers in the world. Our solutions constantly evolve based on the needs of our customers and the direction of their missions. We use an agile approach in solution development, with trained and effective people who have the expertise, the certifications, and the clearances to work in the most demanding and secure environments. We have the tools, people and technology to provide our customers with secure solutions for real-world problems.

Our nation’s interests call for IT security that protects information and communication, assures the identities of users, and defends against threats from internal and external parties.

As threats, vulnerabilities and the strategies for countering them change, Telos responds with new solutions to keep federal and DoD information assets secure. Team leaders and security professionals in all of Telos’ solution areas share expertise and best practices to ensure that all solutions benefit from the latest techniques and technologies for IT security.

Our nation's interests in peace and in war are intimately tied to IT infrastructure. This reality calls for security that protects information and communication, assures the identities of users, and defends against threats from internal and external parties.

Such measures must complement and reinforce one another. They must meet current government and industry standards while also setting the pace for future requirements. And behind these measures, there must be people who apply their expertise to ensure IT security and who respond rapidly and effectively in times of emergency.

Telos is committed to maintaining this level of security and assurance across all our solutions and applications. We invite you to learn more about our people and our work.

Toll-free: 1-800-444-9628

Website: www.telos.com

Twitter: @telosnews

Facebook: facebook.com/teloscorporation

Corporate Headquarters

Telos Corporation
19886 Ashburn Road
Ashburn, VA 20147-2358