# The Cybersecurity First Approach at Comtech

**Cybersecurity must be built into the core culture of an organization if it's going to successfully protect against increasingly sophisticated threats and support the ongoing convergence of global communications infrastructures.**

The secret to success, according to Comtech's Chief Strategy Officer – Defense, Daniel Gizinski, is approaching cyber protection a lot like your daily morning hygiene routine. "Cybersecurity really must become as routine as brushing your teeth or washing your hands," explains Gizinski. "We need to live and breathe cyber hygiene as part of daily operations and not write the challenge off as a few lines of official policy. Skipping cybersecurity for even a day can open the door enough to allow an adversary to walk through."

Comtech's people, processes, and technologies support end users' ability to stay one step ahead to defend against today's most sophisticated cyber threats across commercial, government, and international markets.

In light of recent cyberattacks, government agencies and businesses have become much savvier with their cyber practices and overall security posture. They appreciate more than ever the risk of lost revenue and lost customer trust in the wake of cyber breaches, according to Gizinski. He says government and commercial markets are demanding more cybersecurity discipline and knowledge from their solution and service providers, as they define, design, and deploy security architectures.
"Today's most effective cybersecurity solutions aren't just about hardware, systems and software, they provide an end-to-end view into the security layers required to keep an operation safe today and well into the future," says Gizinski, pointing to Comtech's cybersecurity technology leadership across the company.

## Demand Growing for Smart Flexible Cyber Solutions

The U.S. Government recently ramped up adjustments to its cybersecurity policies with an aim to get out in front of changing risks. Today, cyber threats will only grow as people's daily lives depend more and more on increasingly complex communications networks and services, ranging from cloud technologies, national security operations, Internet of Things (IoT) applications, and access to always-on connectivity, whether you're on an airline or connecting to the internet in a remote region of the world.

At Comtech, cybersecurity and other security features are considered and integrated from the very beginning of the design and development process. The company's security solutions are also designed to readily evolve to stay ahead of the changing threat landscape. "Government, defense and commercial operations are absolutely relying and running on Comtech communications systems and platforms, so they must have adaptable security capabilities built in to meet changing threats," Gizinski explains. Comtech builds software-defined, future-proof cybersecurity into its platforms, enabling customers to easily make security updates to their systems quickly as new threats surface.

"Government and commercial customers can't ship their systems back to us to apply current cyber updates. That's just not feasible," says Gizinski. "Our products have a built-in software-defined architecture that allows the devices to be updated as necessary – easily, remotely and transparently."

We are on the cusp of an unprecedented paradigm shift in cybersecurity as advances in Artificial (AI) Intelligence and Machine Learning (ML) provide opportunities for both bad actors and defensive cyber professionals to automate processes the require a human in the loop today. AI/ML techniques are being used today to adaptively predict threat vectors in advance, enabling proactive, tailored defensive planning. In many cases we've seen advanced defensive techniques that have been able to lead bad actors into walled gardens, turning the tables and enabling cyber researchers to study the threats in a controlled environment.

Comtech contributes to and monitors new military and commercial security standards, including zero trust to network frameworks released by the Department of Defense. The company is consistently ensuring its people, who are developing next-generation solutions and services, are well ahead of the technology curves and well informed on future threats and how to innovate to keep them at bay.

## A Leader in Cyber Training

Comtech not only integrates cybersecurity across its technologies, solutions, and services, but also runs a leading cyber training program to keep the US Government and a wide range of commercial companies ahead of the ever-changing threat landscape. Through **Comtech's CyberStronger** program, the company delivers differentiated cybersecurity services and trainings to commercial and government customers around the world.

"We provide cybersecurity services sought out by intelligence, military, and government security organizations around the world," said Gizinski. "Our technologies ensure our military and government customers have some of the most robust cyber skills and capabilities available to safeguard information and deter adversaries."

Building the cyber resilient workforce of tomorrow is a critical challenge for all organizations, and there's a cyber security skills shortage across the board – 500,000 workers in the US alone and 3.4 million worldwide are needed to develop solutions and combat threats. Drawing on nearly two decades of experience, Comtech is filling today's cyber workforce development gap by delivering the knowledge, skills, and technologies needed to prepare the cyber leaders of today as well as the next generation of cybersecurity experts.

"Comtech has been delivering training for the Department of Defense and other government agencies for decades," explained Gizinski. "We're also providing key training tools and solutions to universities and corporations." Comtech is focused on delivering the knowledge, skills, and abilities (KSAs) necessary for government and corporate employees and teams to perform security roles aligned with the National Institute for Cybersecurity Education (NICE) framework.

As communications infrastructures evolve, this knowledge and Comtech's trainings will be even more important for nearly every commercial and government organization imaginable.

Comtech's commitment to aligning with the DoD Manual 8140.03 and integrating Knowledge, Skills, and Abilities (KSAs) into the qualification process for cyberspace work roles demonstrates their dedication to helping organizations meet the standards for building a more resilient cyber workforce.

The publication of the DoD Manual 8140.03, titled "Cyberspace Workforce Qualification and Management Program," has brought significant changes to how the Department of Defense (DoD) manages its cyber workforce. Comtech's focus on the NICE framework and performance-based assessments aligns well with the new guidelines and enables organizations to meet evolving standards. By integrating KSAs into the qualification process, Comtech ensures individuals possess the necessary theoretical knowledge and practical abilities to address real-world cyber threats. Their emphasis on leveraging technology for tracking, measuring, and managing outcomes further supports the development of a cyber-resilient workforce, making them a trusted partner in building robust cybersecurity capabilities.

Comtech provides performance-based assessment and training using virtual lab environments to measure working knowledge, skills, and abilities. They offer simulated training scenarios where users must perform tasks and solve problems, allowing individuals to gain skills in a practical and accelerated manner. Their training programs have shown high success rates, preparing individuals for job roles with complementary skills to enhance an organization's cyber resilience.

**Contact Us**
**www.comtech.com**

COMTECH™