



professionals and those of our customers.

Today's cyber education has to be more than just an internally-facing objective. At Northrop Grumman, we help customers raise the cyber awareness of their entire workforce to ensure

effective use of policies and procedures. Northrop Grumman is also identifying innovative start-ups and new technologies from both industry and academia that address customer mission requirements and workforce needs.

Northrop Grumman is also committed to building tomorrow's cyber workforce. Partnering with universities and high schools, we sponsor training programs such as the Collegiate Cyber Defense Competition, the Cybersecurity Research Consortium, national cyber Science, Technology, Engineering and Mathematics (STEM) initiatives, and CyberPatriot, a national high school cyber defense competition. The goal is clear: to ensure a robust pipeline of professionals who will secure our nation's cyber future.

Thinking Holistically for Mission Assurance

At Northrop Grumman, we take a holistic approach to cybersecurity, looking at the whole cyber landscape of people, processes and technology and the whole security realm of offense, defense, and exploitation. Thought leadership demands nothing less.

Within our company, we draw on every resource and capability – from information systems and training to advanced platforms and sensors. For our customers, we apply our full understanding of their enterprise and mission requirements and the threat spectrum they face. With Northrop Grumman's holistic approach behind you, cybersecurity is “built in” everywhere. Your information, networks and systems are secure – and driving mission success.

For more information:

www.northropgrumman.com/cybersecurity

To contact us:

cybergroup@ngc.com

Our company plays a strategic role in many industry organizations and international associations. These include the Transglobal Secure Collaboration Program (TSCP), Defense Industrial Base, Internet Security Alliance and others. Our participation promotes the information sharing that is vital to protecting our nation from cybersecurity threats. Partnerships with these organizations are also central to cybersecurity innovation and to furthering the security expertise and effectiveness of cyber professionals.

Grooming Tomorrow's Cyber Workforce

Educating the cyber professionals of today and tomorrow is a responsibility we take seriously. In fact, the cyber workforce is arguably the most important component of cybersecurity.

Continuing to develop the cyber workforce is a top priority at Northrop Grumman. Our cybersecurity professionals on staff are supported by an aggressive workforce development plan. Northrop Grumman's Cyber Academy provides continuous development of our cyber

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN



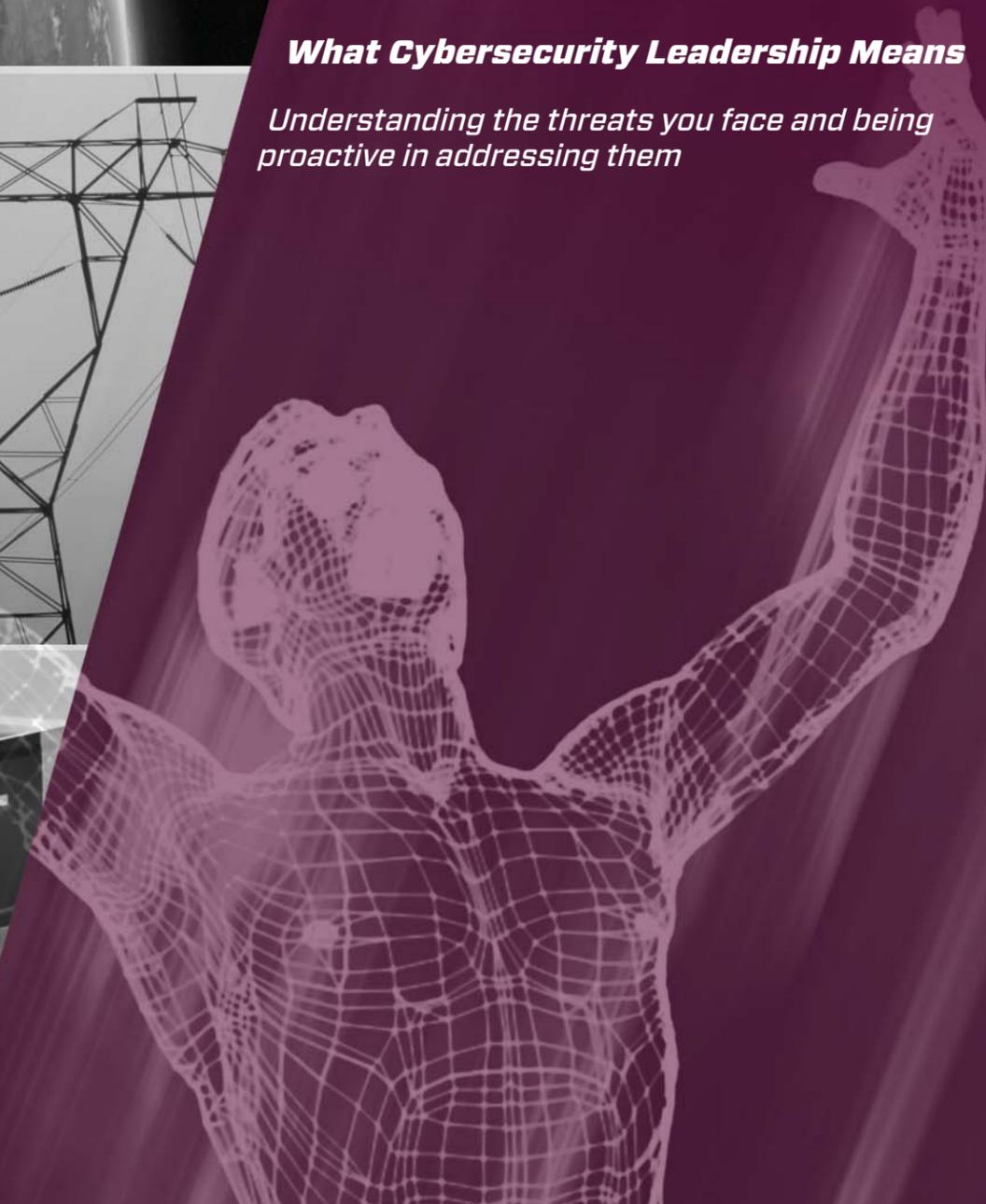
THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

CYBERSECURITY

What Cybersecurity Leadership Means

Understanding the threats you face and being proactive in addressing them



Cyber assets everywhere are under siege from a wide spectrum of threats. Almost daily, these threats grow in sophistication, breadth and speed. Government and commercial enterprises have long been the targets of these attacks. However, the growing reliance on information technology throughout the world's infrastructure has increased security risks to everything from the power grid, satellites, and supply chains to traffic lights and voting machines. Cybersecurity transcends everything we touch.

Assuring the cybersecurity needed for mission success demands agile, enterprise-scale solutions from a demonstrated thought leader. It also requires a rich understanding of the risk and knowing how to leverage experience in both offensive and defensive solutions. To deliver the most effective defensive solution, you must understand how the adversary operates. Success also demands an extensive background in identifying and balancing mission priorities, mission risks, budgets, and regulatory requirements to ultimately keep your enterprise safe.

These are the qualities by which cybersecurity leadership is measured. So what are Northrop Grumman's proven qualities?

Northrop Grumman Leads the Way - Technology, Partnerships and Education

Backed by 20 years of experience, Northrop Grumman is a recognized thought leader and trusted provider of cybersecurity mission solutions. These solutions are establishing the next generation of people, processes and technology that we need to stay ahead of the threat.



Leadership, however, means much more. To stay ahead of increasingly capable adversaries, we look at the whole cybersecurity picture, continually evolving a full-spectrum view of cyberspace operations that brings together capabilities for defense, exploitation and offense. Northrop Grumman is driving innovative research and development, building partnerships across government/academia/industry, and grooming tomorrow's cyber professionals all in an effort to meet the challenge.

Our cybersecurity experience gives us in-depth knowledge of global mission needs across the market. This legacy of experience enables us to more effectively and efficiently align cybersecurity solutions with a wide range of mission and enterprise environments.

Know the Threat Spectrum

Knowing your adversaries and how they operate is key to developing and delivering effective solutions. Cyber threats can come from terrorist groups, foreign governments, crime organizations, industrial spies, hackers and insiders within your enterprise. The sources are often well-funded and organized. The most dangerous risks come from advanced persistent threats, which systematically target your most sensitive and mission

critical information, networks and systems. IT policies, human error, accidents, and supply chains can also be a source of vulnerabilities that can be exploited. Technology changes, while enhancing capability, can affect security throughout organizations. Security has to evolve alongside technology.

Our long history of building defenses against all of these challenges gives Northrop Grumman an unsurpassed understanding of the entire threat spectrum and how to effectively manage your risk. Customers rely on our proven vulnerability and threat analyses to determine their level of risk and to develop the best cybersecurity solutions to meet the need.

Cybersecurity - Built In

Network and system architectures must be flexible enough to allow innovation in response to constantly evolving threats and emerging technologies. Standalone approaches are never enough. Cybersecurity must be proactively "built in" to the full scale and complexity of your enterprise and to every new system and upgrade. To meet this need, Northrop Grumman provides defense-in-depth architectures that combine multiple layers of advanced defenses with the flexibility to accommodate changing cyber policies, tech-

nologies and threats. And as a leader in agile software development and acquisition, we build cybersecurity into each "cycle" as we rapidly roll out new technology.

Northrop Grumman developed "The FAN™," our layered cybersecurity defensive reference model, to serve as a baseline for customers building a secure IT architecture that will keep data safe. Applying The FAN establishes architectures with integrated layers of protection for perimeter, network, endpoint, application and data security. The model incorporates prevention, testing and policy management, plus complete operational support, including continuous monitoring and incident response.

Innovative Solutions - Secure By Design

How much security is enough? Do I have highly trained people, defined processes and agile technology? What innovations will address the cyber threats I face? Can I trust them to work? Will they deliver the protection to assure the mission?

To answer questions like these, Northrop Grumman has made aggressive technology investments in key research areas, such as identity management, situational awareness, model-

ing and simulation, cloud security and supply chain. And by design, we build cybersecurity into all our systems and processes from the beginning. This saves on lifecycle costs and protects our customers from expensive system modifications to meet the evolving threats.

To accomplish this, we leverage our world-class facilities where we develop and validate technologies and solutions. Northrop Grumman's CyberSpace Solutions Center provides a powerful research and development resource for concept exploration, capabilities development and mission execution in high-fidelity replications of actual network environments. The federated U.S. and U.K. cyber ranges offer a robust emulation environment for developing and testing mission-integrated cyber technologies as well as for training cyber professionals. Northrop Grumman's Cyber Security Operations Center protects our company and our customers' cyber assets worldwide. TRIAD, our global network of advanced cyber laboratories, provides a high-bandwidth platform for cybersecurity research in large-scale network environments.

Cybersecurity innovation and thought leadership are not just about technology. Building strong partnerships and grooming a skilled cyber workforce are essential.

Partnerships for Research and Information Sharing

A significant part of thought leadership derives from partnerships with the most important sources of cybersecurity expertise. These partnerships drive critical research, demonstrate practical solutions and support invaluable opportunities for information sharing and collaboration.

Northrop Grumman joined with MIT, Purdue and Carnegie Mellon to form the Cybersecurity Research Consortium and tackle major cyber problems like attribution and supply chain risk. We support research initiatives with small businesses and more than 100 universities. The Technology Incubator is a partnership with the University of Maryland Baltimore Campus and a link to innovative start-ups and new technology.

We take a holistic approach to cybersecurity, looking at the whole cyber landscape of people, processes and technology