



Cybersecurity:

Program Managers Have Questions.
Got Answers?

Brian Brodfuehrer

Cybersecurity is an area where program managers (PMs) find themselves between opposing forces. It is clear to them that cybersecurity is important and needs to have their attention, but where does it fit with all the other program priorities that have to be worked up front and early? What exactly should they be putting their attention on, and how? The kind of information they need on the subject is in the middle too; it is not at the national strategic policy level (although that affects them), and it is not in knowing the latest virus, back-door weakness or technology advance (but that is an impact too).

More than 2 years ago, the Defense Systems Management College of the Defense Acquisition University began to pull more cyber-related information into its executive-level education programs. We developed a disguised cyber-based dilemma case study called *Greyhawk UAV* and piloted an elective titled *Cybersecurity for Program*

Brodfuehrer is a faculty member in DAU's PMT-401 course. He has more than 30 years of acquisition experience, working for both the government and industry.

Managers which remains a work in process. As a faculty member, I began to ask my students: "What is one thing you wished you knew about cybersecurity?" The military and civilian students were from military Services, government agencies, and the defense industry. They were a mix of Level III certified O-5/6 and GS-14/15 acquisition professionals with an average of more than 10 years of experience. Over the past 2 years, I collected many questions and have now grouped them into theme areas.

This article is more about sharing the questions than about answering them. I will, though, share a few tips I have collected that are of value to PMs. I am interested in developing a continuing dialogue on cybersecurity, tailored for PMs. To that end, DAU is looking to establish an online community of practice on the NIPR and SIPR network environments. The goal is to have an ongoing forum where PMs can ask questions and where cybersecurity experts can help with answers that will work for the program managers.

Shaping the Cyber-Question Landscape: A Framework for Analysis

Approximately 150 questions were collected and grouped into theme areas. These theme areas were then arranged in an acquisition-focused landscape with the program manager at the center. This framework provides a first insight into how to go about answering the questions and how to teach the material to future students. (See Fig. 1.)

In the center of the figure are the PMs and their key stakeholders. Their job is to make progress along the acquisition process to get the system into the user's hands at the lowest reasonable cost. The PM is ultimately trying to make wise use of scarce taxpayer resources to quickly get the best value product to those in harm's way. From the PM view in the center, every-

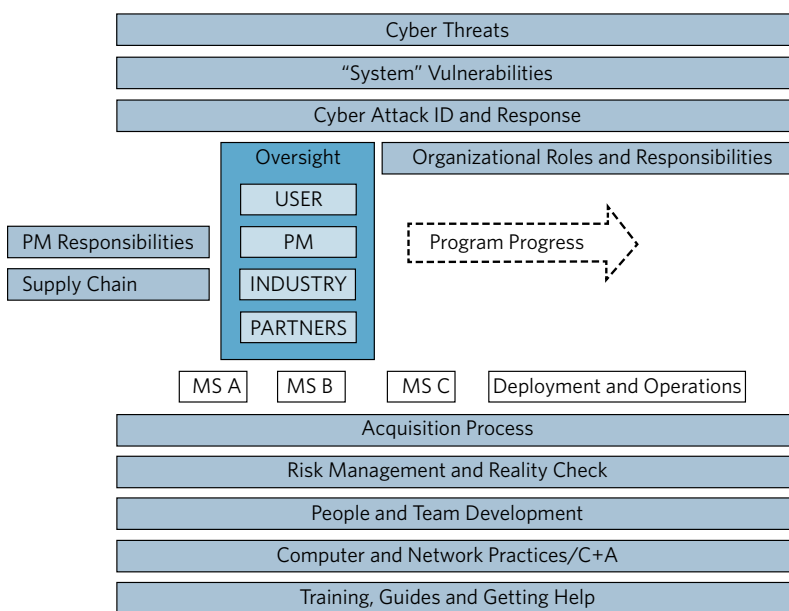
thing else can be viewed as a strength, weakness, opportunity, or threat to getting that job done. Program managers' cyber concerns overlay the whole acquisition process and they need to understand and have access to resources and tools to help mitigate the concerns.

The PM questions covered both pre-attack and post-attack scenarios with the latter causing the most concern. Looking at the figure, cyberattacks can come from external or internal actors and can exploit any vulnerabilities in the system. By "system," I mean the big picture, including the people, process, and products across the acquisition lifecycle. When a cyber threat exploits those system vulnerabilities, the attack should be identified and a response created to mitigate the attack. Program managers want to know the best way to go about doing that. But, they were also concerned about how to do the proper planning necessary to avoid an exploitation. Those questions were captured in the figure under the other blocks: organizational roles and responsibilities, PM responsibilities, supply chain, acquisition process and milestone requirements, risk management (including a reality check), people and team development, improved computer and network security practices, certification and accreditation, training, PM cyber guides, and getting help from subject matter experts. PM questions about cybersecurity span the life cycle, and the action to design a robust system will likely depend on the operational CONOPS, the information and access that need protection, the system vulnerabilities, and the threat and nature of the potential attack.

Questions and Tips

Below are listed typical questions from about 2 years of student inputs. Over this time I have also collected tips for PMs dealing with the cyber area. The tips are not intended to be full answers to the questions; they are just the best I have at this time.

Figure 1. PM Cyber Landscape



Threats

What is the scope of potential cyberattacks as a whole and what methods are used most frequently?

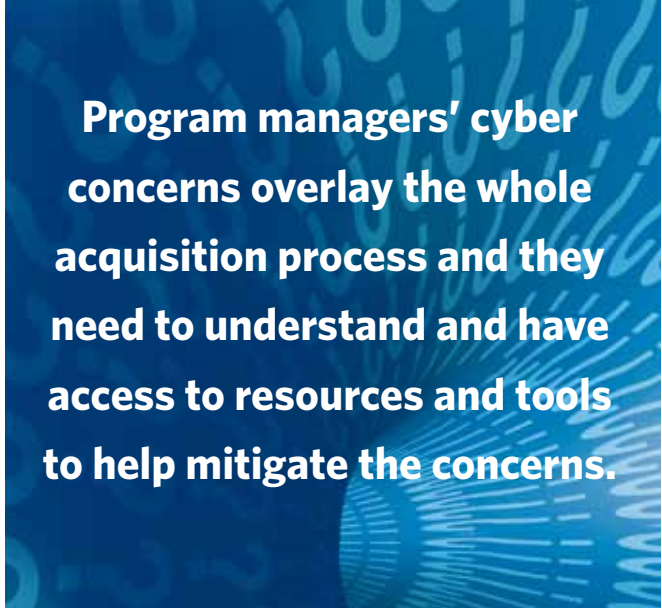
What is the biggest cyber threat that should concern program managers?

What are the latest (emerging) threats to DoD networks?

Is there a government organization responsible for assessing the threat? How do I interface with that organization?

Vulnerabilities

How do I determine how vulnerable my program is? How do I minimize the danger of compromise? Are there tools, techniques, or processes to assess system vulnerabilities?



Program managers' cyber concerns overlay the whole acquisition process and they need to understand and have access to resources and tools to help mitigate the concerns.

What is the process for obtaining a vulnerability assessment and how do I get periodic assessments?

Tip: Know what you need to protect; it may be more (or even different) than what you expect.

Tip: Do not discount the value of unclassified information. When separate bits of unclassified information are pieced together, they can produce a story that may reveal sensitive or even classified information.

Attack Identification and Response

How are cyber-attacks identified and reported within the military services?

Can you provide response strategies and approaches for different scenarios such as attacks being directed at: the government program office, a government partner, the prime contractor, a subcontractor, a vendor or an operational system? A step by step process for how to deal with potential breaches would be helpful.

Are there mandatory reporting requirements? What are the triggering events, processes to follow, timelines to be used in following the processes and names of individuals and organizations to contact?

How would I or one of my industry partners know we are under attack? What do I do, whom do I talk with if my team suspects an attack or breach?

How do I assess and monitor the threats, vulnerabilities and security across a large, multi-vendor program?

If I am working in a cloud environment (government or commercially based cloud) how can I be alerted to an attack that might impact my program? Would response processes differ from a non-cloud environment?

Organizational Roles and Responsibilities

What is the chain of command for cybersecurity in the different Services? For example in the Navy there is a Naval Net Warfare Command and a new Cyber Fleet Command. What are their roles and responsibilities? Again, how is cyber split up in the other Services that have similar cyber commands?

How do program managers, Services, organizations combine resources to counter the threats?

Who has overall jurisdiction when a cyber-event happens in a program management office or in a related industry partner?

What resources are available, knowledgeable and willing to help in this field? I have heard of organizations like: Defense Cyber Crime Center (DC3), Damage Assessment Management Office (DAMO), Chief Information Security Officer (CISO), Defense Industrial Base Collaborative Information

Sharing Environment (DISCE). Can you describe their roles and capabilities and how to contact them?

Is there a list of key points of contact, phone numbers, and e-mail addresses to contact, either to obtain help or to report a problem?

Can you provide a specific process for notification of compromises and the AT&L (Acquisition) organizations responsible?

Tip: Know the people (and organizations) that can be helpful.

Tip: Each Service branch deals with cyber in a different way. If you work on a joint program, don't assume that just because you classify something as CPI, another branch will do the same. Also, don't assume everyone on a joint program is following the same processes required by your branch of Service.

PM Responsibilities

What authorities and limitations does a PM have for establishing and enforcing cyber requirements?

What documents should a PM use to plan for cybersecurity? And how does the planning flow to the contractor supply chain?

Is there contracting language or lessons learned available to help?

What cybersecurity issues could slow or stop a program?

Tip: Ensure everyone, including your leadership, realizes they are accountable for cybersecurity.

Tip: Communicate across systems and functional boundaries. IT systems owners need to talk with mission systems owners and security pros with software developers, for example. The boundaries are often connected. Expertise on both sides is needed to effectively work the problems but they don't naturally communicate.

The PM must work the people side. Create, encourage and reward those cybersecurity-professional 'heroes' who are inclined to learn the technology and the problems and work to create operationally sensible solutions and policies.

Supply Chain

Is there a list of trusted hardware, integrated circuit and software foundries/developers? Are there any regulatory requirements on software, middleware, hardware and integrated circuits?

Is there a mechanism in place to quickly evaluate all subcontractors throughout the supply chain? How do I set up and maintain a cost-effective plan for supply-chain security management?

What are key vulnerabilities to be aware of when buying commercial parts?

Tip: Ensure industry partners are aware of and working to minimize threats throughout the acquisition lifecycle.

Acquisition Process and Milestone Requirements

What makes a good program protection plan (PPP)? Are there examples and templates?

How is critical program information (CPI) determined? Are there tried and effective methods for determining CPI? What are the important occasions for updating the CPI list?

What cyber-related documentation and information is required at different milestone gates? Who on the service and OSD staffs gives the OK to the documentation work that has been accomplished?

What are best practices for planning before the inevitable cybersecurity issue arises? Is there an acquisition phase based approach for the best practices?

Tip: The program protection plan is a tool in your cyber risk management toolbox. Don't just push it through the process; spend time preparing it, and get the right people working on it with you.

Risk Management

How do you determine the best tradeoff between usability and security?

What is an objective standard for deciding how to balance "protection" with "over-reaction" and the resulting costs?

Tip: Cyberthreats cannot be totally mitigated: You must manage the risk!

Reality check

What are the truly effective countermeasures vs. the things we throw our money away on?

What is the prevalence of cybersecurity incidences that impact program offices?

What are the "real" threats out there?

People and Team Development

How do I ensure my staff, especially systems engineering and security personnel, are properly trained to consider information assurance throughout the system architecture and life cycle?

Our program security folks are mostly trained and involved with physical security. How do I help them transition to understanding and working on cybersecurity?

Is there a DAU or other DoD organization career field (or series of courses related to cybersecurity)? Is cybersecurity seen by DoD as an acquisition competency?

Tip: The PM must work the people side. Create, encourage and reward those cybersecurity-professional "heroes" who are inclined to learn the technology and the problems and work to create operationally sensible solutions and policies. Heroes are not the rock throwers (those who point out problems and do nothing to solve them). Drive for consensus among the experts so that the team can move forward to accomplish something.

Tip: Every time you (or one of your staff) logs into an IT system, consider yourself "at war."

Improved Computer and Network Security Practices

What is the latest thinking on whether longer passwords really make us more secure?

How do I make cyberdefense undetectable to the attacker and low-impact to the operational effectiveness of the organizations and users of the systems?

How do I measure the effectiveness of the cyberprotection approaches my program has in place?

How do I translate abstract concepts to concrete steps to defend information without breaking my budget and without coming across as a dictator in seeking and obtaining alignment with the other program “up front and early” swim lanes?

Certification and Accreditation (C+A)

What is the correct process for obtaining the necessary DoD approvals for network connectivity for NIPR and SIPR?

How do I work C+A for a system that crosses Services or agencies? How do I obtain system certification by one agency that will be recognized by another one?

Training

What training is available to assist PMs with cybersecurity as it relates to programs?

Tip: Your policies are no stronger than the weakest link on your team. Take advantage of every opportunity to educate and train your staff on cybersecurity.

PM Cyber Guides

Is there an information card with phone numbers to call?

Is there a book or guide: *Cybersecurity, a PM Guide to Success?*

What are the simple things the PM can do to protect government and contractor networks?

Are there checklists or tools to determine areas of weakness of a program protection plan?

Getting Help


What organizations provide cybersecurity protection for government programs?

What subject matter expert support outside our agency is available to help?

What are the latest tools, technologies and techniques for cybersecurity?

Where can I access government or contractor expertise to assist the PMO in identifying CPI and how to effectively and economically protect it?

What's Next?

This article is intended to start an ongoing dialogue that will identify questions program managers have about cybersecurity and establish a source for answers. There is also another important question that the larger community can help answer: “What questions should we be asking, but are not?” By sharing the questions and setting up a forum to discuss them and their answers, DAU can raise awareness of the threat and of ways to protect the nation’s acquisition programs. 

The author can be reached at: brian.brodhuehrer@dau.mil.

ACQUIPEDIA

ACQUISITION ENCYCLOPEDIA OF COMMON TERMS

An online encyclopedia that provides the acquisition workforce with quick access to information on common acquisition topics and terms.

Online articles provide just what you need to know in a **succinct and digestible format:**

- **Definitions and narratives**
- **Links to related policy, guidance, lessons learned, tools, communities, training, and other resources**

Your reference tool for acquisition topics

- **Quick**
- **Concise**
- **High-value content**
- **Searchable**
- **Available 24/7—when and where you need it**



[HTTPS://ACC.DAU.MIL/ACQUIPEDIA/INDEX.HTM](https://acc.dau.mil/acquikipedia/index.htm)