# Implementing Cybersecurity into an Existing National Nuclear Non-Proliferation ProgramME – A Case Study

R. ANDERSON

Idaho National Laboratory

Idaho Falls, Idaho, United States

Email: address@correspondingauthor.com

R. HOFFMAN

Idaho National Laboratory

Idaho Falls, Idaho, United States

S. GODWIN

Pacific Northwest National Laboratory

Richland, Washington, United States

D.S. VANDYKE

Pacific Northwest National Laboratory

Richland, Washington, United States

**Abstract**

Cyber threat profiling and risk mitigation is critical to any nuclear state organization and should be considered as part of any comprehensive nuclear security programme. Defining and evaluating the impact of the cyber threat to mission can be challenging. An existing national nuclear non-proliferation organization undertook an effort to incorporate computer security activities into its programme to address cyber risk. One of the primary goals of this endeavour was to develop a set of prioritised recommendations for organizational follow-through. The organization dedicated subject matter expert resources in the form of a cyber task force to support this goal. Opportunities were identified where computer security could be built into each programme including office-level strategies and tools. Of course, no new identified threat vector is easily considered and incorporated into existing programmes without impact. There are many obstacles to be overcome. Technically literate subject matter experts are difficult to find, management has comparatively less experience applying computer security into its programmes, and trying to change the culture to consider computer security risk at policy and programmatic levels takes time and management attention. As an outcome of this process, a roadmap for program integration was developed, including the establishment of a cyber support team. This paper will discuss the challenges and successes associated with establishing such a team.

## INTRODUCTION

Computer security threat profiling and risk mitigation is critical to any nuclear state organization and should be considered as part of any comprehensive nuclear security programme. Defining and evaluating the impact of the cyber threat to an organization’s mission can be challenging.

It is critical that computer security be included in an organization’s vulnerably, risk, and impact considerations and decisions. It can be challenging to establish and evolve a team to address and incorporate computer threat.

Challenges to implementing a computer security programme include:

1. Scarce talent pool: Technically literate subject matter experts (SMEs) are difficult to find.
2. Management inexperience or lack of knowledge: Management tends to have less experience with computer security than other security functions in their nuclear security programme.
3. Culture change: Trying to change culture surrounding computer security takes time and management engagement in order to communicate the critical need for computer security as equal to other security concerns.

To complicate this further, computer security typically has not been integrated into organizations’ leadership, policy, procedure, staff understanding, and culture to the level that physical security has. Without rigorous and comprehensive attention to computer security, an organization exposes itself to significant risk. Many organizations are beginning to understand and address computer security in their organization but may lack the ability to plan and implement the necessary changes.

The U.S. Department of Energy, National Nuclear Security Administration, Office of Defense Nuclear Non-proliferation (DNN) found itself facing a similar challenge and worked with Idaho National Laboratory (INL) and Pacific Northwest National Laboratory (PNNL) to plan and implement change. A computer security support team (CST) was created to help DNN bridge the gaps they have in computer security within their deployment programmes. This paper will explain how DNN is implementing computer security into an existing National Nuclear Non-Proliferation Programme. This paper will also describe how this solution was created, evolved, and the plans to continue addressing the computer security needs of DNN as it moves forward against a backdrop of dynamic cyber threat.

### Establishing the Need

The DNN works with international and domestic partners to secure, safeguard, and dispose of dangerous nuclear and radiological material, and to detect and control the proliferation of related weapons of mass destruction technology and expertise. To accomplish this mission, DNN develops policies, programmes, technologies, and digital assets that deliver significant benefits and protection. Similarly, nuclear and radiological facilities worldwide are increasingly adopting digital components into their security, safety, and operational systems. These digitised systems have greatly improved efficiency monitoring and control of nuclear and radiological operations. However, they can also manipulate vulnerabilities that adversaries might target to gain system, network or even physical access to sites. As has been underscored by repeated high-profile cyber intrusions, cyberspace is a contested environment and attacks are increasing in frequency and sophistication.

Although DNN senior leadership recognised the potential of cyber threat impacting mission they had no means to quantify the severity. Reaching out to SMEs from several U.S. national laboratories, an exhaustive self-assessment was performed that identified pervasive gaps in several computer security related areas and provided justification for formation of a dedicated cyber resource within the organization.

The CST formed to assist DNN address the changing computer security environment. INL and PNNL senior leadership was key to the CST’s origins. Computer security SMEs helped senior DNN leadership understand the need for computer security and created a genesis of momentum.

While many organizations get as far as recognising risks and threats, change would not have been possible without the support of a senior leader in DNN. With the support of this senior leader, the seeds of the CST were planted. DNN recognised it needed assistance; PNNL and INL agreed to work alongside DNN leadership and staff to partner toward computer security sustainability.

Note that the CST formed was not to work with the classic information technology teams, as those teams were within the purview of DNN’s chief information officer. The CST’s purpose was to help the DNN staff working on deployed programmes and projects.

Throughout this paper, key factors will be highlighted for each stage of the process.

Key Factors:

* Designate and use a senior leader as a champion;
* Get assistance from computer security experts who will work collaboratively with your organization;
* Recognise that existing enterprise information security office was only responsible for desktop computing and not more nuclear-centric cyber threat challenges facing the organization.

### Forming the Team

The CST formed as a partnership between a small group of DNN and national laboratory staff. This partnership allowed the cyber experts at the national laboratories access to DNN programmes for evaluation and support.

The CST was composed of core and adjunct members. Core members were DNN-designated leadership and national laboratory experts that could serve as advisors and leaders for the adjunct members. National laboratory-based core members consisted of a project manager and deputy project manager from each laboratory.

Adjunct CST members from the labs were SMEs in computer security that the core team could call on for support. Instrumental in the success of adjunct CST members was the expectation of relationship building within DNN programmes and the enhancement of team capabilities in specific subdiscipline area such as; reactor control design, physical security systems, facility assessments, technical education, sensor development etc. Another important component to the adjunct CST relationship with offices was the fact that they were not there to disrupt programme/operations or take budget away. These adjunct members were assigned to programmes and offices within DNN and acted as trusted agents that could be called upon by the DNN teams for assistance and support.

Key Factors:

* Engage a champion in your organization supported up by SME leads;
* Expect SMEs to develop trust and relationships within the programmes and offices;
* Ensure team members have both the cyber and programmatic operational experience necessary to deliver credible solutions.

### Establishing Objectives

After the CST was assembled, it developed a set of prioritised recommendations for organizational follow-through. The draft recommendations were created following individual meetings between core members and DNN leadership. Those meetings both disseminated the purpose of the CST and gathered a baseline of capabilities and knowledge within the organization. These individual meetings were also used to request leadership’s permission to let adjunct members meet with and interview DNN team members.

Following these exploratory meetings, the CST baselined their objectives and was formally chartered. The objectives came directly from what was learned on the exploratory meetings and was tailored to fit the DNN mission. The objectives of the CST became threefold:

1. improve cyber awareness within DNN (grow a sustainable cyber culture).
2. support DNN programmes to integrate computer security into their activities thereby identifying cyber risk to mission and effectively mitigating that risk.
3. provide interagency policy leadership and strengthen interagency coordination.
4. reduce cyber risk at the DNN policy level.

### Working with the Offices

To get a baseline understanding of computer security maturity across the DNN organization, two adjunct subject matter expert members met with each of the four DNN subordinate offices over a few months. The adjunct members met with various staff, including senior leaders, individual deployment project managers, and support organization members (e.g., contracts and travel).

The CST worked with individual programme offices to understand how the cyber and nuclear threat landscape was evolving, how it impacted each office, and how and where DNN should consider further action to reduce risk. The CST also began to support programme offices with development, SME resourcing, and implementation of international computer security outreach strategies and provide cross-DNN visibility into programme initiatives and consistency of computer security approach.

At this point, another issue arose—the demand for computer security experts exceeded the supply (common to many organizations attempting to plan and integrate computer security concepts--both internal and external to the organization and in the products offered to partner countries). The CST became an informal coordinator of computer security SMEs throughout DNN programme offices.

Key Factors:

* Require SMEs meet individually with DNN staff members to understand the computer security maturity of your organization;
* Require CST leadership to prioritise and coordinate SME resources.

### Assisting the Offices

Once the team had been organized, chartered, and objectives were created and verified by DNN staff members, the adjunct CST members began to operate as trusted agents within DNN programme office teams. This method produced three success stories.

1. One team helped review and mitigate risk for an existing multi-year technical project.
2. A second team was instrumental in evaluating and implementing change to a large programmatic hardware deployment.
3. A third team integrated with the team conducting remote training and evaluations of partner country systems.

These early successes were due largely to leadership support and trust built between adjunct CST members and DNN program office staff.

A significant challenge that the CST helped identify and solve was staff education in computer security. Many nuclear non-proliferation organizations have strong and established physical security knowledge and experience. That knowledge needs to be complemented with computer security to create a comprehensive understanding of risk and vulnerabilities. To address this need, the CST provided the following training to improve the knowledge and application of computer security across DNN.

* **Awareness Training**: Curriculum was designed to deliberately remove ineffective training mediums and cumbersome elements. The CST used instructional system design experts to focus on knowledge transfer and retention. Minimising a dependence on slide decks and maximising collaborative exercises and hands-on activities were core to course development. Four courses were created and deployed:
	+ - * **101: Computer Security Basics**.

This course presents students a base understanding of what a cyber threat is and how it can impact an organization. The course provides scenarios and activities to involve students in decision making, including a capstone game where students decide how to invest in protecting organizations and then see the results of those decisions. The intended audience for this half-day course includes directors, programme and project managers, and project staff. Learning outcomes include the ability for students to recognise cyber threats to their organizations and proactively begin to mitigate the risks.

* + - * **201: Computer Security- Where Do I Start?**

This course augments the 101: Computer Security Basics course by delving deeper into the DNN mission space, investigating how computer security applies, and outlining the first critical steps to applying computer security mitigation/principles into the various mission activities. The intended audience for this half-day class includes directors, programme and project managers, and project staff. Learning outcomes include the ability for students to identify computer security challenges in their area of responsibility and provide general programmatic- and project-level guidance.

* + - * **202: Building Computer Security Requirements into New and Existing Programmes**

Digital devices have permeated all aspects of our lives adding efficiencies, capabilities and enhancements. Unfortunately, these same devices have exposed us to new risks. This course helps students understand how these risks to programme activities can be mitigated through risk-informed policy, contracting language, and design requirements and computer security-specific specifications. The intended audience for this half-day class includes programme and project managers, acquisition professionals, and contract specialists. Learning outcomes include the ability for students to recognise where computer security controls and requirements are appropriate and include computer security requirements in relevant plans and programmes.

* + - * **204: Computer Security Assessments: Where, When and Why?**

Computer security assessments can vary widely from conversations and document reviews, to destructive analysis of digital devices. Each type of assessment has value and can answer various questions. This course helps participants understand various types of assessments and the questions each can answer. The intended audience for this one-day class includes programme and project managers. Learning outcomes include the ability for students to understand goals and activities in computer security assessments, identify assessments applicable to their mission space, and be able to converse about assessments with partner countries and organizations.

* **Monthly Threat Briefs**: SMEs within the CST created monthly threat briefs to highlight key computer security events relevant to DNN’s mission. Current events in operational technology computer security are reviewed and lessons learned pointed out to DNN staff.
* **Computers Security Speaker Series**: To augment the interactive courses, the team recruited outside industry experts to speak about key computer security events relevant to DNN’s mission and provide DNN staff with insight from industry security experts and other government organizations.
* **CST Website**: The internal website was created to be a single hub for CST and computer security-related information. It also includes a calendar of events and training resources of interest to DNN staff.

This set of engagement and education mediums provided a range of learning opportunities to personalise the training experience. Each experience was created to address a specific need and educate staff on risks in nuclear non-proliferation computer security.

Key Factors:

* Create tailored and sustainable knowledge transfer and training opportunities for staff by using instructional design professionals and multiple mediums of learning.

### Working toward Sustainability

Lastly, the DNN CST established itself as a leader in U.S. interagency efforts to promote consistency and improve computer and nuclear security practices internationally. The CST supported a National Security Council-founded interagency coordination group intended to foster interagency collaboration and communication on this important topic.

This CST model proved successful in delivering valuable input to DNN computer security efforts. These efforts have shifted culture and critical thinking at DNN toward incorporating computer security into planning, risk decisions, and implementation of deployment programmes.

As this shift occurs, the CST recognised that it must adapt and evolve too. The CST is currently changing its approach to remain relevant, effective, and sustainable. Changes include the following:

* CST leadership is transitioning to a rotating assignment within each programme office rather than remaining at the DNN front office. This change offers more leadership exposure to computer security needs and risks, accountability a level closer to the work being done, and an opportunity to become better embedded in the culture of the offices and programmes.
* A Computer Security Council, made up of DNN programme and office representatives, has been created. The CST will help administer the council; however, the intent is for the individual DNN offices and programmes to take responsibility for incorporating and reporting on computer security-related activities. This also provides DNN representatives a forum for coordination and collaboration.
* An “Aide De Camp” added to the team to help with awareness, logistics and coordination.
* A plan to hire federal staff with computer security backgrounds. To be fully sustainable, qualified staff will be needed. DNN is working to hire leadership-level individuals to coordinate computer security activities and mid-career and early career computer security staff members.



*FIG. 1. Sustainable CST Structure*

These CST changes in approach will help DNN to further embrace computer security as a risk that must be evaluated and addressed.

Key Factors:

* Adapt your approach to address the evolution of your programme’s progress.

## CONCLUSION

The CST has grown in three phases to address the needs of DNN.

### Building the Foundation

During the first phase of CST, lab SMEs worked with DNN leadership to educate them about computer security and worked to understand how DNN functioned. The SMEs were able to see what DNN security posture looked like. The CST was then chartered and created a set of prioritised recommendations for organizational follow-through and dedicated subject matter expert resources in the form of a cyber task force to support that goal.

### Engaging the Community

The second phase was to embed SMEs with the offices and programmes. SMEs worked to identify opportunities where computer security could be embedded into each programme, including office-level strategies and tools.

### Sustaining the Team

The third phase was to adapt to further success by helping DNN implement sustainable computer security.

This paper describes a successful example that other organizations can emulate. It can help other national nuclear non-proliferation organization incorporate computer security activities into their programmes to address cyber risk. This paper also offers anecdotal evidence to guide an organization through a similar transition. To address this and summarise the lessons learned from the creation, execution, and evolution of the CST, here are the key factors again:

Key Factors:

* Designate and use a senior leader as a champion;
* Get assistance from computer security experts who will work collaboratively with your organization;
* Recognise that existing enterprise information security office was only responsible for desktop computing and not more nuclear-centric cyber threat challenges facing the organization;
* Engage a champion in your organization supported up by SME leads;
* Expect SMES to develop trust and relationships within the programmes and offices;
* Ensure team members have both the cyber and programmatic operational experience necessary to deliver credible solutions;
* Require SMEs meet individually with DNN staff members to understand the computer security maturity of your organization;
* Require CST leadership to prioritise and coordinate SME resources;
* Create tailored and sustainable knowledge transfer and training opportunities for staff by using instructional design professionals and multiple mediums of learning;
* Adapt your approach to address the evolution of your programme’s progress.

As non-proliferation and nuclear state organizations look to bolster their computer security programmes, they may find that the organization needs help to begin and implement the needed changes.

No approach is perfect, and each organization has its own challenges. The approach described above could be a template to help your organization get past the first hurdle of engagement and into productive risk evaluation and mitigation. Soon your organization will make strides toward a sustainable approach to computer security.

ACKNOWLEDGEMENTS

The U.S. Department of Energy, National Nuclear Security Administration, Office of Defense Nuclear Non-proliferation (DNN) has been gracious enough to allow their CST to be used as an example for this paper and we are grateful for their willingness to share openly that others may learn.