cybersecurity education

# APPLICATION OF PEDAGOGICAL FUNDAMENTALS FOR THE HOLISTIC DEVELOPMENT OF CYBERSECURITY PROFESSIONALS

Barbara E. Endicott-Popovsky
and Viatcheslav M. Popovsky

Nowhere is the problem of lack of human capital more keenly felt than in the field of cybersecurity where the numbers and quality of well-trained graduates are woefully lacking [10]. In 2005, the National Academy of Sciences indicted the US education system as the culprit contributing to deficiencies in our technical workforce, sounding the alarm that we are at risk of losing our competitive edge [14]. While the government has made cybersecurity education a national priority, seeking to stimulate university and community college production of information assurance (IA) expertise, they still have thousands of IA jobs going unfilled. The big question for the last decade [17] has been 'where will we find the talent we need?' In this article, we describe one university's approach to begin addressing this problem and discuss an innovative curricular model that holistically develops future cybersecurity professionals.

## CYBERSECURITY EDUCATION: HOW IT STARTED

Both the National Security Agency (NSA) and the Department of Homeland Security (DHS) have launched programs to increase production of cybersecurity experts. In the late 1990s the National IA Education and Training Program (NIETP) was formed to manage Information Assurance (IA) education and training at the Federal level. NIETP supports the Committee on National Security Systems (CNSS) in the executive branch, which, among other duties, sets national-level IA training standards. NIETP has a number of active programs, among which are:

- **Centers of Academic Excellence in IA Education program (CAE/IAE)** Jointly sponsored by the NSA and DHS, this program promotes university and community college involvement in IA education and research by designating Centers of Academic Excellence that meet certain criteria [15]. Currently, there are 166 CAEs in 42 states, the District of Columbia and the Commonwealth of Puerto Rico.
- **Colloquium for Information Systems Security Education (CISSE)** Formed in 1997, CISSE provides a forum for IA leaders in government, industry and academia to define requirements for IA education and to encourage expansion of IA curriculum at institutions of higher learning.
- **National Information Assurance Training and Education Center (NIATEC)** NIATEC is a consortium of academic, industry and government organizations that detail training standards and maintain a library of IA curriculum materials that map to those standards. Under the leadership of Idaho State University's Dr. Corey Schou, one of the founders of NIETP, NIATEC maintains ties to ISC2, considered the global not-for-profit leader in 'gold standard' IA certifications.

NIETP provides a foundation to dramatically increase the population of prepared cybersecurity experts; however, to date, the production has fallen short of filling the tens of thousands of jobs that are going vacant [3,8]. The need has burgeoned in recent years.

cybersecurity education

# Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals

## INCENTIVE PROGRAMS: ENCOURAGING IA STUDENTS

To encourage students to pursue IA government careers, in 2000, the White House issued the Federal Cyber Services (FCS) training and education initiative. This initiative included the very successful *Cybercorps: Scholarship for Service* (SFS) program that authorizes funding of up to 300 undergrad and graduate students each year through programs awarded by the National Science Foundation (NSF) to a subset of competing CAE/IAE's [26]. Each scholarship recipient signs a contract to work for the government upon graduation—one year for every year of scholarship received. The Department of Defense (DoD) offers a similar program, the Information Assurance Scholarship Program (IASP), designed to attract students into DoD IA careers. Awardees sign agreements to work for DoD agencies upon graduation. IASP funds approximately 200 students at any one time [4].

While incredible incentives, doing the math, these programs combined do not begin to reach the employee numbers government needs, even if the SFS program had been funded for a full complement of 300 students each year—and it has not. Add the needs of industry, and conditions translate into a war for talent [14].

Not only are the numbers insufficient, but, given the evolution of the threat spectrum over the last decade from young people seeking street cred to determined cybercriminals and nation states, the depth of knowledge of current graduates is being questioned by the government agencies and industries hiring them. It is not unusual to hear comments at conferences from government officials and industry leaders like 'we are creating a lot of frequent flyers, but not many pilots,' or we are unhappy with the 'check-list security people' produced by academia—implying that a one-size-fits-all, recipe approach to curriculum dominates these programs. Besides more numbers, we need IA graduates with problem-solving skills and out-of-the-box thinking abilities that many employers aren't seeing.

### The Pedagogical Question

While NSA and DHS policies have been successful in 1) generating IA curriculum standards through robust dialogue among industry, government and academia and 2) encouraging universities and community colleges to teach IA curriculum that maps to these standards, producing greater numbers of IA graduates than we would have otherwise. We also need a pedagogical methodology and approach that will generate the creative problem solvers we want. The question is not just 'where do we find them,' but also 'how do we efficiently produce creative, problem-solving IA graduates with the requisite skills and expertise our employers require?' It has become a quality concern.

Over the last decade, this question has intrigued us. At the University of Washington's (UW) Center for Information Assurance and Cybersecurity (CIAC), we have developed conceptual and operational pedagogical models that help us begin to tackle the question of how to produce problem-solving IA experts in the short amount of time we have them as students. This is still an evolving work as we continue to elaborate our approach and share our insights. We are hopeful that our models and examples may be useful to other institutions addressing the same question. We would welcome a dialogue with others who wish to share their perspectives, as well.

### The CAE/IAE as a Pedagogical System

From the beginning, we conceived of the CIAC as a pedagogical system designed to produce IA professionals from incoming students—at the meta level, we viewed them as raw material to be processed! A unique blending of Russian and American pedagogical approaches [12,20,27] resulted in the authors creating the KBP (Kuzmina-Bespalko-Popovsky) Pedagogical model (Figure 1)[1] that represents the CIAC pedagogical system taking in raw student talent and producing IA expertise as outcomes. This model was first introduced by the authors in 2008 [18] and is considered a high-level metasystem model that, when applied to developing a specific course, produces a specific instantiation of the model referred to as an Information Assurance Curriculum (IAC) system model, several of which have been outlined in previous publications [5, 6, 7].

[1] This operational pedagogical system is derived from intensive research into two schools of thought regarding the theory of pedagogical systems whose originators are Dr. N.V. Kuzmina and Dr. V.P. Bespalko, respectively. In acknowledgement of the body of work of these two distinguished academics, whose main models we have integrated and modified, we called our model Kuzmina-Bespalko-Popovsky (KBP).

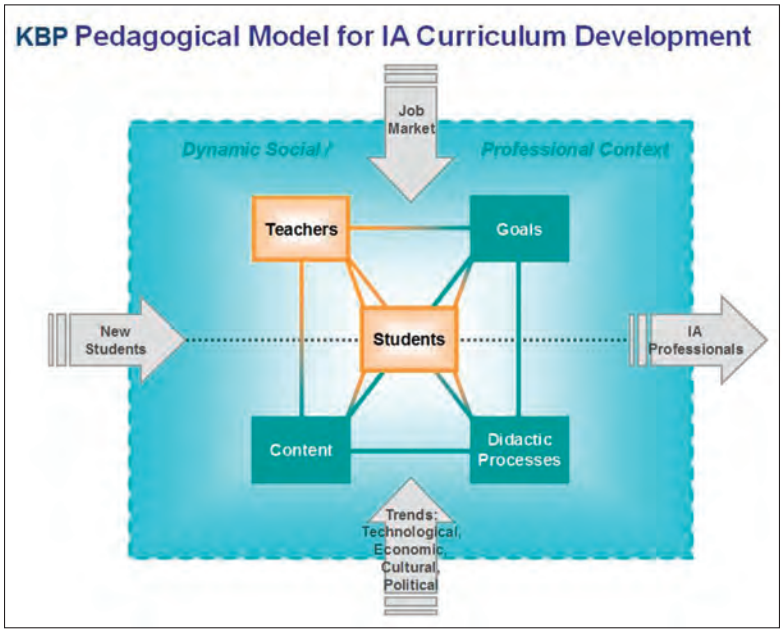



Figure 1: The KBP Pedagogical Model: CIAC as a pedagogical system

The KBP is composed of five model elements—*students, teachers, goals, content* and *didactic processes*—the first two of which are intelligent elements, the *teacher* and the *student*; the remaining three are infrastructure elements—the *goals*, *content*, and *didactic processes* of the curriculum. All elements of the model are dynamic, subject to varying rates of change and adaptation. All of the elements of the model function as an interconnected whole. They operate within a larger dynamic professional and social context that includes economic and political environments, as well as a constantly evolving set of threats, vulnerabilities and operational systems that are affected by influences such as global competition; technological innovation; legal policies; and the creativity of business leaders, entrepreneurs and IA specialists. This context informs the different elements of the model.

In any given context, a specific instructor with his/her own specific slice of IA knowledge and expertise is responsible for developing a specific set of infrastructure components designed to address the needs of a specific type of student.

*Students* are central to the model—entering the system as potential IA employees; exiting as IA professionals.

By describing each component of the model in relation to learning objectives drawn from the environment and an integration of trends and the condition of the job market, an educational plan is developed iteratively. According to Bespalko and Kuzmina, the more precisely the five components are characterized—along with the connections among them—the more repeatable and predictable the learning results [1,12].

The five elements interact and are changing constantly. Over time, as each of the elements is changed, it affects the other four, requiring each of them to be redefined, and so on, until all five elements are specified in relation to one another. By continuously updating descriptions of these elements, curriculum is kept current ensuring that students remain competitive. We have our curriculum on an annual review cycle, using the model to help us think through curricular changes.

To help envision this process, each of the five elements is elaborated in a later section in relation to one IAC, but first we review the guiding principles that have infused the curriculum development process we use.

## Guiding Principles

When we apply the KBP model to developing courses, we operate under the guidance of five key principles that are considered every step of course development.

**Guiding Principle 1:**
**System Activity-based Approach to Learning**

According to Michailova [13] and Talizina [24], system activity-based learning is a holistic process that combines learning and productive activities directed toward developing professional abilities and motivation. In this approach, knowledge is not a goal in and of itself, but a remedy for solving practical problems [13,19,21, 24]. The outcome is professional and personal maturity, creativity, the ability to organize one's continuing education as a professional, and student contributions to the community, industry and academia. The center has adopted the system activity-based approach to learning as fundamental to the professional preparation of our students. This approach is characterized by the following five elements:

**a) Learning through productive activities**

Activities are developed in partnership with an active Northwest cybersecurity community. This includes real world projects and capstones as student assignments. Students present their work to a professional audience and receive honest feedback. *All* participants in these activities—government and industry leaders, university instructors and students, and cybersecurity experts—engage in the learning process, promoting learning from one another.

**b) Motivating students to learn on their own**

We expect students to become lifelong learners, taking responsibility for their own professional development beyond the classroom, if they wish careers in IA. It is characteristic of a professional that they stay current in their field. This is especially true for the fast moving field of IA where those who succeed develop their own methods of staying current: creating a regimen of daily readings, becoming active in professional organizations, consciously building a network of collaborators that they can draw on. Students are advised to do the same.

Motivating students to learn on their own plays out in the curriculum in assignments that encourage students to

- Develop their own dashboard of RSS-fed, security readings from the internet
- Attend local workshops and conferences held by the regional cybersecurity community that is active and large.

Throughout the course, we tell students that we expect them to become lifelong learners.

**c) Knowledge is only a tool, not an end**

Gaining knowledge is not the end goal (i.e., learning for a grade), but is a tool to solve practical, complex problems, creatively and independently, unleashing the learner's potential. While we test students to establish a measure of knowledge acquisition, the bigger emphasis is on creative application of what they know to solving unstructured real world problems.

**d) Personal and professional development as outcome**

Personal and professional development is the end goal. We expect students to exhibit creativity and professionalism in their work and be highly motivated to learn continuously and independently. In many cases, this requires students to transform from being a consumer of whatever the professor provides, to taking an active role in their own personal development. Tools to enable personal growth become part of the curriculum like learning to reflect on their own and others' practical experience to extrapolate generalizations through inductive reasoning.

Character and ethics are discussed in relation to personal and professional growth as students assume responsibility for maintaining currency as an obligation to clients and employers to provide the best possible and most current solutions to their IA problems.

cybersecurity education

## Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals

**e) Real measures of actual production**

Criteria for measuring the efficiency of this educational approach are the actual contributions to science and industry made because of cooperative activities. Students are expected to write papers worthy of publication (undergraduates as well as graduates), compose meaningful reports to 'clients,' solve industry problems and effectively present results to business leaders.

This system activity-based approach is adaptive in nature. The five fundamentals mentioned above are a foundation of the educational work of the Center, allowing students to stay current and teachers to move rapidly to adjust curriculum to new learning objectives as the dynamic environment in which we are working changes.

### Guiding Principle 2: Mini-max 'brick' Approach to Curriculum

From the beginning, we recognized that there wasn't sufficient time to teach everything that students need to know about IA, nor would that even be feasible. The body of knowledge is forming, expanding, and is not universally agreed upon. It covers a large number of disciplines; students will likely specialize. We know no one who would claim to know everything in IA, and would be suspect of anyone who said they did. The challenge we faced in developing curriculum was to teach enough knowledge on the subject in order for the student to take it from there and succeed on their own professionally.

The solution requires judicious selection of topics from a much larger body of knowledge and decisions about how much time out of the quarter to devote to each topic. Further, in order to ensure students are dedicated enough to assume the initiative to continue to learn on their own, we need to select interesting topics and assignments that we know will engage them. Digital forensics, for example, with all of the attention CSI receives in popular television programs, is a topic that intrigues students. Exercises in identity theft—such as dumpster diving, war walking and google-hacking—also engage student interest, getting them excited about the subject.

Applying the Mini-Max model for teaching IA (Figure 2), we identify the content topics in IA we wish to cover for a particular course, in relation to the other four elements of the pedagogical model, and then identify where those topics fall in the continuum described in Figure 3 (Levels of Learning). The 'brick' (colored block) represents the totality of the IA body of knowledge (BOK); the slice through the 'brick' represents that minimal part of the BOK that must, in our judgment, be taught in the course. Some topics deserve only a mention—in other words, a well-educated IA professional would at least recognize the term or concept. Others are more important to emphasize and are candidates for productive, as opposed to reproductive, learning, that is, lab experiments, participation in research, problem solving in a real-world environment.

Later, we will walk you through the model presented in Figure 3 to show how it is applied in a curriculum development example.

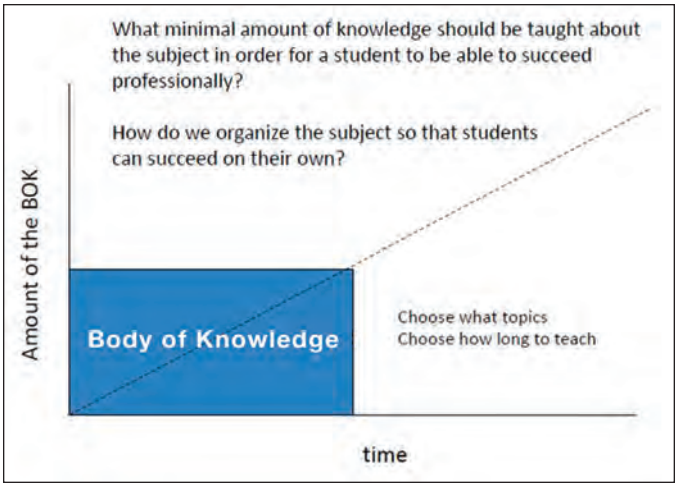



Figure 2: Mini-Max Model for Teaching a Subject

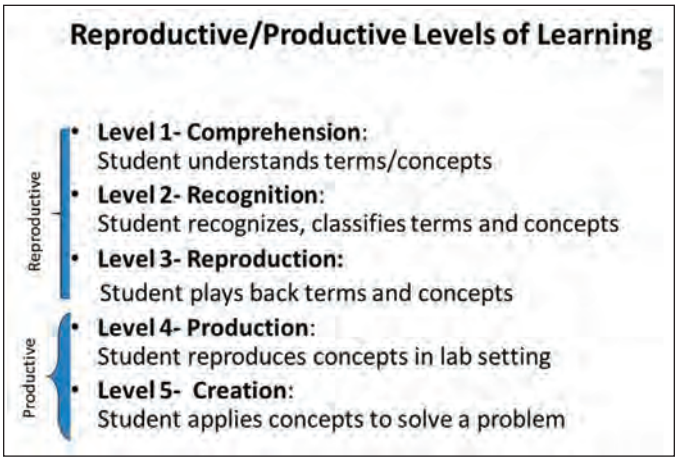



Figure 3: Levels of Learning: Palette of Pedagogical Options (Source: V.P. Bespalko [1])

### Guiding Principle 3: IA as a Toolkit, Not a Recipe

We teach IA controls as a set of tools, frameworks and solutions to be mixed and matched to the specifics of an organization, as opposed to focusing on any one particular approach. We did so out of necessity to meet the employment needs of our region (many different approaches are used in practice); fallout from this approach is that students learn there is no one recipe.

In the early years of the Center, unlike many CAE/IAE's, we responded more to local industry demands for graduates than to the Federal government. In a study we found that the majority of graduates ended up working within 30 miles of the university, an area dominated by industry. At the time, Microsoft had launched the Trustworthy Computing initiative [9]; Boeing was actively seeking IA employees; local companies, like IO Active (pen testers), were asking for resumes of students familiar with IA and secure coding. With the impetus coming more from industry, we emphasized using a variety of standards and tools adapted in a variety of ways to suit the different environments and circumstances of local employers, as opposed to focusing on Federal government IA standards—although these are covered. Since compliance regimes

have grown up within industry sectors, they often overlap within organizations that must comply with a variety of standards—such as PCI, HIPAA, GLBA, SOX—producing hybrid models. We prepare our students to be able to create IA plans in such mix and match environments.

This has shaped our approach to curriculum. While using Federal training standards as the baseline, by training our students in a variety of tools, they are quickly disabused of the notion of a single IA 'recipe' being appropriate for all. That makes them uncomfortable at first; but they learn to problem solve. In designing our courses, this principle manifests, for example, in our reliance on actual cases presented by guest lecturers from industry and government, reinforcing the idea of an IA toolkit, as opposed to expecting a formula. We compare IA experts to plumbers who come to the house with a variety of tools—some they will use, some they won't need—depending on the problem they uncover.

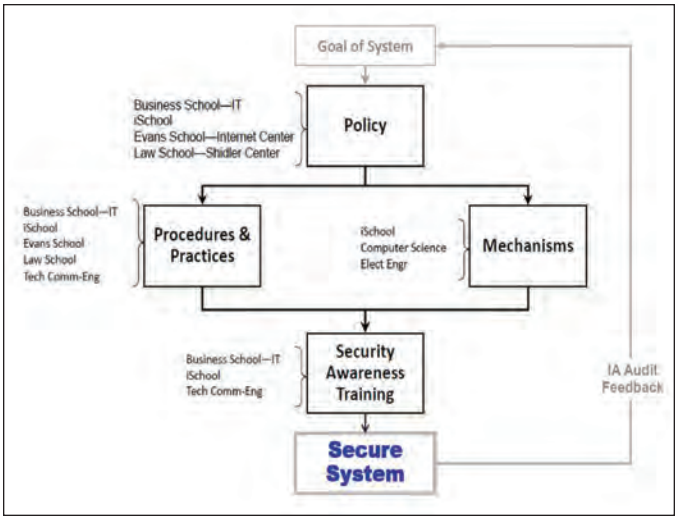



Figure 5: Multi-Disciplinary Approach to Information Assurance

**Guiding Principle 4:**
**Cross Sector and Interdisciplinary Approach**

From the beginning, we stressed regional collaboration across sectors (Figure 4), forming Center collaborations with various government, academic and industry organizations. This is expressed in the curriculum in several ways: we make frequent use of guest lecturers from these sources; take on real-world problems as class projects and capstones; and facilitate internships with government and industry, as well as research collaborations with other universities—foreign and domestic—that include our students. Solving complex, real-world problems stretches them to use their IA knowledge in productive, as opposed to reproductive, ways (Figure 3).

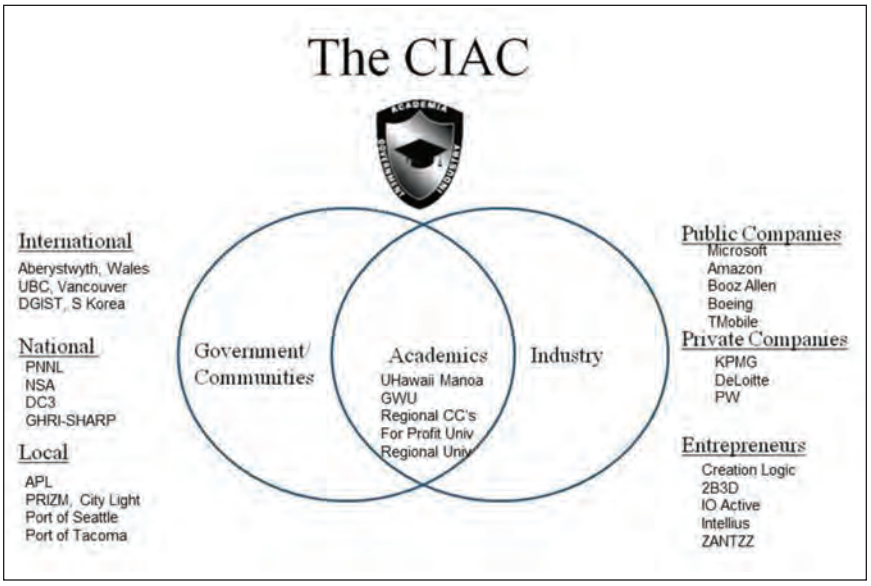



Figure 4: The CIAC: Integrating Community, Industry and Academia in the Pacific Northwest

We also stress a cross disciplinary approach to IA. Taking an organizational view of IA from the Chief Information Security Officer (CISO)'s vantage point, we produced the model in Figure 5 that has guided curriculum development in different academic disciplines at the university. Recognizing that elements ranging from policy to technology keep information secure, we can take a business school slice, for example, through the model, emphasizing the management aspects of IA—policy, compliance procedures, developing an organizational culture of security through awareness training . Using this model, we have developed IA curriculum for business, computer science, information science, library science and urban planning programs—all drawing from the same organizational/operational view of security shown in Figure 5; each taking a relevant slice of this picture that aligns with their particular discipline.

**Guiding Principle 5:**
**Analogy to Developing Elite Athletes**

From inception, we analogized the challenge of optimizing development of 'cyber warriors' with the development of Olympic athletes, drawing extensively on the work and experience of one of the authors who was involved with selection and preparation of elite athletes and sport educators for high performance athletic teams [19,25].[2] He applied all of the above approaches while a professor at the prestigious St. Petersburg Lesgaft State University, Russia, the oldest academy of its kind, famous for maturing coaching and athletic talent for Russian national sport and Olympic teams. His work has been disseminated extensively inside and outside Russia in the sports industry and beyond.

We anticipated that by assessing students upon entering our pedagogical system and tai-

[2] Cyber warriors is a term we apply to both industry and government cybersecurity experts. The internet makes no distinctions, in the attackers' view, among the sectors. They are all targets

cybersecurity education



loring curriculum to their specific needs, engagement would increase, as well as interest in IA. This in turn would accelerate learning and ultimately the development of expertise. We have begun to see career results in our graduates that lead us to believe this is supportable. We are in the process of data collection that will allow more discrete analysis of our results.

The meta model in Figure 6 summarizes our pedagogical management approach, beginning with assessment, then making relevant decisions about deficiencies and remedies that translate into execution of resulting plans, and then providing feedback for program correction. When optimizing the development of an elite athlete, the coach (or educator) carefully assesses the skills and capabilities of each athlete, diagnosing strengths and deficiencies, making decisions and executing plans designed to nurture strengths and compensate for deficiencies, then entering into a feedback loop that results in re-assessment. Likewise, in our view, developing elite cyber warriors requires the same approach.

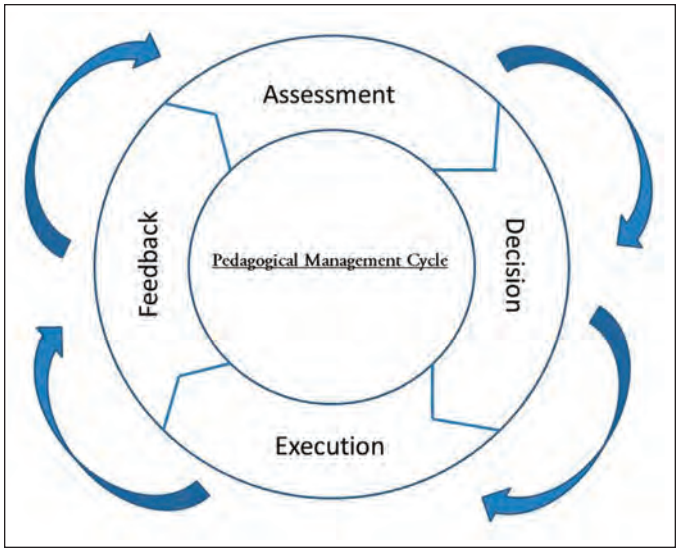



Figure 6: Pedagogical Management Cycle

We use this model to assess and plan for an entire incoming IA class, characterizing the incoming cohort so that we can tailor our offerings to engage them. That means each year, with each new IA cohort, the curriculum varies. Each incoming group is asked the following series of questions:

- In what degree program are you enrolled?
- How close are you to graduation?
- What is your background in IA (knowledge and experience)?
- What do you wish to get from this course (besides a good grade!)?

From our experience, aside from the obvious differences implied by each discipline in which our courses are taught, each new cohort has a distinct character. Answers to these questions at the beginning of the year are used to assess their level of readiness for studying IA and the curiosities that drive the group. This information results in adjustments to the curriculum content to meet the needs of these particular students, keeping in mind our pedagogic goals.

To enhance our management approach, as a systems forming factor, we now employ the NIST/NICE model to encourage students to do their own personal assessment and guide their own growth beyond what they are getting in class.[3] The job tasks associated with each NIST/NICE pathway help students determine the kinds of things they might enjoy doing on the job. The associated skills required for each pathway provide students with a template for understanding what they need to know in order to be qualified for the pathways that interest them. They can compare this list with what they are learning in their formal IA classes and seek remedies outside the program to complete what they need to know. Remedies include professional organization membership, certifications, internships, research projects, reading—things they must do themselves, outside the classroom, in order to complete their preparation as professionals for the track/s they choose to pursue.

This is just the beginning of the student's transformational process and only partially addresses content delivered. The complete pedagogical system we designed provides an efficient path to IA professionalism, from raw recruit to competent practitioner, putting the student at the center of the process. We put these pieces together through an example that follows.

## EXAMPLE IAC: SECURE SOFTWARE CODE DEVELOPMENT CURRICULUM (SSCD)

Secure software code development curriculum (SSCD) is one example of an IAC instantiation derived from the KBP pedagogical model. Given the economic and employment environment in the Pacific Northwest in the middle of the last decade when local employers placed new emphasis on the production and deployment of secure software code, we became interested in preparing our students to meet these new demands.

The problem we were presented by industry was compelling. The same programming flaws in code were being created over and over, in spite of raised awareness at the workplace and availability of public tools like the NVD (National Vulnerability Database) and the CWE (Common Weakness Enumeration) that catalogue software flaws. Employers encouraged us to teach secure coding practices as one way to mitigate the problem in our graduates.

Applying our model, we created a pedagogy designed to enhance the professional preparation of software engineers, making them more competitive in the marketplace, and enabling them to carry an inherent sensitivity to the security consequences of the software they build. We have been working with this original IAC system ever since in subsequent iterations, in addition to developing and disseminating curricular artifacts and workshops to assist

[3] The NIST/NICE framework [16] provides useful guidance to government, and now industry, in describing careers in cybersecurity. As educators, we have found it useful guidance in identifying educational outcomes.

other faculty in developing secure coding courses and threaded topics for insertion in existing classes.

## Applying the KBP model

Using our approach, we first described each element of the KBP at a high level—Students, Teachers, Goals, Content, and Didactic Processes—and how they interrelate.

The **Students** in the initial instantiation of the SSCD were professional software developers who needed to unlearn their coding habits and re-learn new secure software coding techniques. The in multiple modes—kinesthetically, as well as aurally and visually.

Applying the KBP Pedagogical Model to create the SSCD-IAC (information assurance curriculum) model, the same two generic intelligent elements and three generic infrastructure elements persist and then must be specifically described in terms of secure software code development. The five elements of the KBP function as a system; changes in one element will induce changes in the other four, and so on. Thus instances of the SSCD-IAC model will vary, for example, with changes in the students. What we might teach returning adults with development experience will differ

**Within the software engineering community, there is an increasing recognition that secure coding practices are only a subset of the activities needed to create secure information systems.**

**Teachers** were experienced software developers with a background in secure code development who could bring actual cases and examples from their practice into the classroom.

In walking through the remaining infrastructure elements, we have the following.

## Goals

The overall goal was to induce learning within a mature set of students, causing a change in behavior. This is different from working with students who are just learning programming. Our students needed to change long-held ways of thinking about coding and adopt new programming habits. Thus, learning objectives incorporated individual personal and professional growth ideas in addition to the new technical skills and knowledge that students were expected to master. Understanding the goals of the class for this specific set of students helped prioritize learning objectives assigned to each lesson, which were based on information assurance and secure coding best practices. These learning objectives included things like: understand and explain IA principles and practices, understand and demonstrate threat-modeling techniques, implement secure coding techniques, produce systems that protect information.

## Content

Content for a secure software code class was drawn from a large body of knowledge that integrated standards produced by recognized software development groups and subject matter experts. Specific content was tailored to fit into the available class time and mapped to course goals. Further, a range of learning levels and skills to be acquired were mapped to the class content and sequence of presentation. This will be discussed in more detail later.

## Didactic Processes

How we teach is as important in our model as the content. Didactic processes used to deliver content in the secure software curriculum were selected to match learning goals related to the content elements in the course. For example, hands-on case studies were used to emphasize certain topics so that students were stimulated to learn from what and how we might teach undergraduates with no programming experience. During the actual curriculum development process, these five elements were exhaustively discussed among the collaborators. We've just touched on some of the changes that may distinguish one instance of the SSCD from another. As the curriculum is developed through the process discussed next, these elements are revisited and changed iteratively as the curriculum continues to be defined and described.

Conceiving of curriculum as an inter-related system of elements has eased the process of updating IA curriculum to reflect the dynamic changes the field experiences. It has also eased the development of IA curriculum for different disciplines, enabling us to produce new adaptations efficiently.

## Methodology for curriculum design

According to Bespalko's methodology for curriculum design [1], the six steps below must be followed in the order presented:

1) Determine the content of the subject in light of general educational goals.
2) Determine specific goals (levels of learning) for each element of the subject taught.
3) Determine in what order each element of the content should be taught.
4) Determine the amount of time to be spent on each subject and optimize the student's progression through the subject, teaching the minimum needed to be able to perform independently.
5) Define methods of control/evaluation based on goals for each subject element.
6) Recommend the didactic processes that teachers can use.

Next, we describe developing the SSCD following the six steps and produce artifacts we developed during the process.

**Step 1:**
**Determine content considering educational goals**

We chose the Asset Protection Model as the basis for curriculum content. The authors, co-developers of the APM (Figure 7), view

cybersecurity education

## Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals

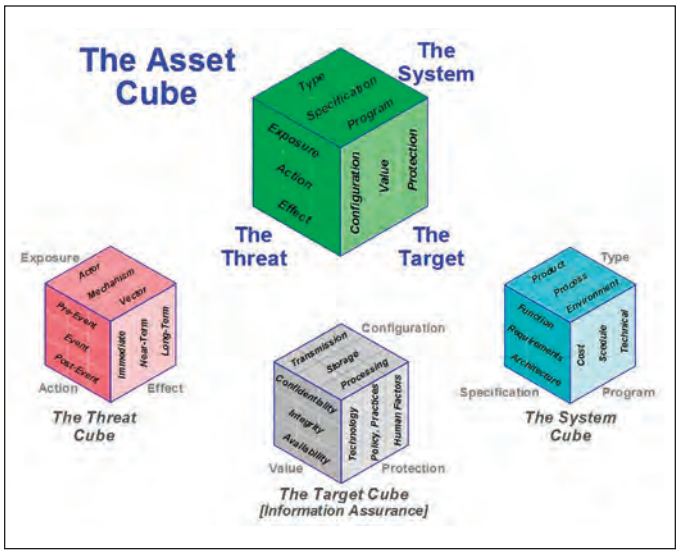



Figure 7: Content Source: Asset Protection Model (APM)

this model as a comprehensive source for secure code curriculum topics [11,23,25]. It provides a common conceptual ontology for secure information system topics; a stable logical framework that is independent of specific organizations, technologies and their associated changes; and a vehicle for structured communication among these groups.

Within the software engineering community, there is an increasing recognition that secure coding practices are only a subset of the activities needed to create secure information systems. Not only the software, but also the hardware, networks and people that contribute to those systems should be considered. The APM accommodates this.

The model acknowledges that the practice of secure information systems design, development, deployment and operation is shared by three professional communities: the justice and intelligence communities, the information assurance community, and the systems engineering (including software engineering) community.[4] Each community is represented in Figure 7, respectively, as: the threat cube, the target cube and the system cube, providing a focus for each community.

Using these three cubes as a reference, topics for secure code curriculum were selected and a graph hierarchy, showing relationships among them, was developed (Figure 8). From the graph, a logical outline of topics was created (Figure 9). Note that the names of the elements evolved as we worked through the process.

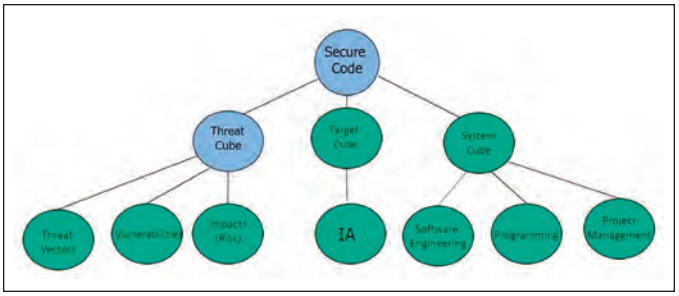



Figure 8: Graph Model of Content

Subsequent steps in the methodology are based on this artifact.

### Step 2: Determine specific goals (levels of learning)[5]

Each secure code topic must be assigned a level of learning the instructors believe it deserves in the curriculum in the context of the course goals. As an example, under the *Target Cube, 2.2 Policy and Procedures* may be taught at no greater than a Level 2 or 3. The student either recognizes the term or is able to discuss it in class and perhaps write about it, reflectively. On the other hand, under the *Product Cube, 2.1 Secure Design Patterns and Practices*, since the curriculum goal is to make better software engineers, it makes sense that this topic becomes a focus of more intense learning Levels 4 or 5. To give the reader a sense of what is required at each level, a comparison of *Learning Level III: Reproduction and Learning Level IV: Production* appears in Figures 10. Note the differences in activities required of each.

I. Threat Cube
- 1.1. Threat Vector
  - 1.1.1 Deception
  - 1.1.2. Theft
  - 1.1.3. Manipulation
- 1.2. Vulnerability
- 1.3. Impact

II. Product Cube
1. Development Processes
   - 1.1. Secure Development Lifecycles
   - 1.2. Project Management
   - 1.3. Security in Artifacts
2. Programming
   - 2.1. Secure Design Patterns and Practices
   - 2.2. Language and Compiler Considerations
   - 2.3. Technology Considerations
3. Quality Assurance
   - 3.1. Static Analysis
   - 3.2. Dynamic Testing
   - 3.3. Penetration Testing

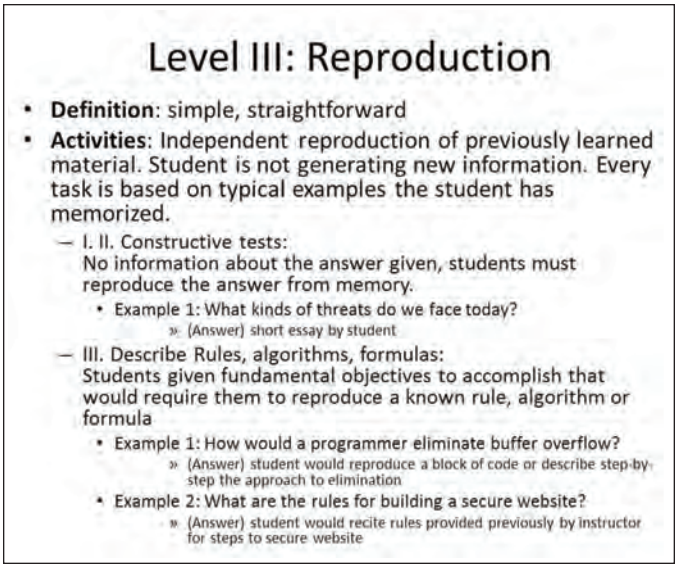
III. Target Cube
1. Security Services
   - 1.1. Confidentiality
   - 1.2. Integrity
   - 1.3. Availability
2. Security Countermeasures
   - 2.1. Human Factors
   - 2.2. Policy, Procedures
   - 2.3. Tools
3. Information States
   - 3.1. Transmission
   - 3.2. Processing
   - 3.3. Storage

Figure 9: Logical Outline of Secure Code Curriculum Topics

The output for Step 2 is a table that lists curriculum elements and provides the Level of Learning associated with each. Table 1 provides a sample from the course topic outline above. Levels of Learning can be assigned at whatever level of detail time allows.

[4] The APM integrates several models like: the SSE-CMM (Systems Security Engineering-Capability Maturity Model), the OWASP Software Assurance Maturity Model; output from the NIST/DHW SwA working group; the Microsoft Security Development Lifecycle, the Project Management Body of Knowledge (PMBOK), and the McCumber cube.

[5] Bloom's Taxonomy [2] addresses levels of learning as well, although we rely on Bespalko [1] and Kuzmina [12].



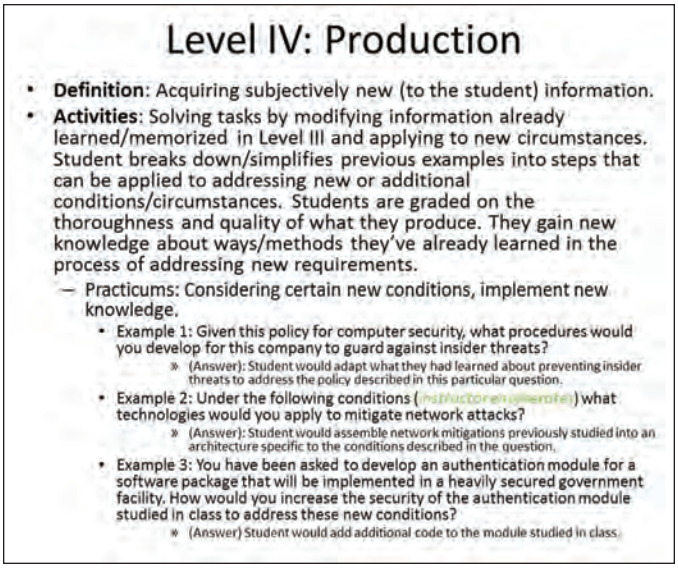




Figure 10: Learning Level III vs. Level IV

**TABLE 1:**
**SAMPLE CURRICULUM ELEMENTS VS. LEVEL OF LEARNING**

| Threat Cube | Topic | Learning Level |
|---|---|---|
| 1.1 Threat Vector | 1.1.1 Deception | Level 4- Reproduces in lab |
| | 1.1.2 Theft | Level 4- Reproduces in lab |
| | 1.1.3 Manipulation | Level 5- Solves a problem |
| 1.2 Vulnerability | | Level 3- Plays back info |

**Step 3:**
**Determine order each element of content should be taught**
Once levels of learning have been established, topics are organized in the order they should be taught. For our purposes, we were designing not just one course, but a series of topics and courses in secure coding that could be taught across multiple years. We decomposed the elements in further granularity and then distributed them across a four-year program. The first year's activity is given in Figure 11.

**Step 4:**
**Determine the amount of time to be spent on each subject**
This step is straightforward. Total classroom hours are distributed across the course topics. Figure 12 is work product that indicates where time will be spent in the first course. Emphasis was on orientation to IA (Target Cube), with more time spent on the Threat Cube.

Each step in the methodology produces dialogue among the instructor/collaborators. This helps enrich the end product and prepare several instructors to teach the material.

**Step 5:**
**Define methods of control/evaluation based on goals for each subject element**
At this stage, we identified assignments that would elucidate each topic. Going back to our guiding principles, our preference was for

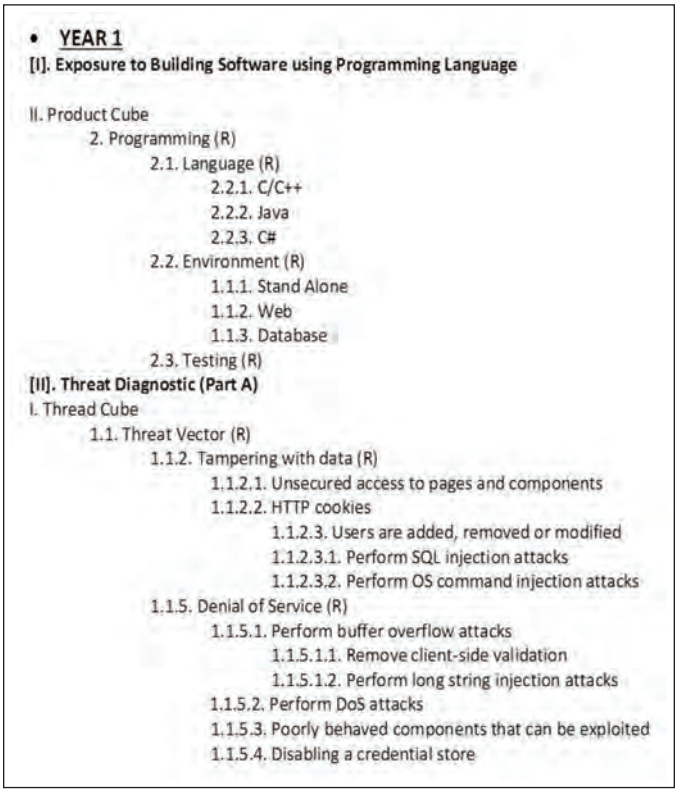



Figure 11: Part of Year 1 of Secure Code Curriculum Plan

activity-based learning. We identified exercises that could be either demonstrated in the lab or performed as a homework assignment, depending on how we chose to evaluate students. 'Deception' and 'Theft' were categorized as Level IV learning opportunities indicating exercises that could be performed in a lab setting with instructor guidance (Figure 13). 'Manipulation,' not shown here, was identified for exercises in creative problem solving which meant either partnering with 'clients' on a real world problem or perhaps developing a demonstration on their own to share with the class.

cybersecurity education

# Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals

- **I. Threat Cube**
  - 1.1. Threat Vector
    - 1.1.1 Deception (8)
    - 1.1.2. Theft (14)
    - 1.1.3. Manipulation (13)
  - 1.2. Vulnerability (3)
  - 1.3. Impact (3)
- **II. Product Cube**
  1. Development Processes
     - 1.1. Secure Development Lifecycles
     - 1.2. Project Management
     - 1.3. Security in Artifacts
  2. Programming
     - 2.1. Secure Design Patterns and Practices
     - 2.2. Language and Compiler Considerations
     - 2.3. Technology Considerations
  3. Quality Assurance
     - 3.1. Static Analysis
     - 3.2. Dynamic Testing
     - 3.3. Penetration Testing
- **III. Target Cube**
  1. Security Services (3)
     - 1.1. Confidentiality
     - 1.2. Integrity
     - 1.3. Availability
  2. Security Countermeasures (11)
     - 2.1. Human Factors
     - 2.2. Policy, Procedures
     - 2.3. Tools
  3. Information States (3)
     - 3.1. Transmission
     - 3.2. Processing
     - 3.3. Storage

Figure 12: Topics with Assigned Hours

- **I. Threat Cube**
  - 1.1. Threat Vector
    - 1.1.1 Deception (8)
      - 1.1.1.1. Spoofing identity
        - 1.1.1.1.1. Basic HTTP Authentication sends credentials in the clear
        - 1.1.1.1.2. Credentials of tokens stored in HTTP cookies
        - 1.1.1.1.3. Authentication tokens in the clear on the wire
        - 1.1.1.1.4. Intercepting DNS request – DNS spoofing
      - 1.1.1.2. Repudiation
        - 1.1.1.2.1. User performs illegal operation and there is no trace of what happened
        - 1.1.1.2.2. Attackers get a product ordered w/o paying and there is no audit trail
    - 1.1.2. Theft (14)
      - 1.1.2.1. Information Disclosure
        - 1.1.2.1.1. Reading on the wire
        - 1.1.2.1.2. Error messages at login time divulge too much information
        - 1.1.2.1.3. Unsecured pages and components
      - 1.1.2.2. Elevation of Privilege
        - 1.1.2.2.1. Hijack someone else's session
          - 1.1.2.2.1.1. Perform cross-site scripting attacks
          - 1.1.2.2.1. 1. Sniff the session ID using a network sniffer
        - 1.1.2.2.2. Replay a stolen session
        - 1.1.2.2.3. Log in without the proper credentials
          - 1.1.2.2.3.1. Perform SQL injection
          - 1.1.2.2.3.2. Perform brute-force / dictionary attacks
        - 1.1.2.2.4. Use forceful browsing to access pages with no proper authentication
          - 1.1.2.2.4.1. Use URL tampering techniques

Figure 13: Topics with Assignments

Topics at lower levels (1 – 3) would be subject to evaluation on written tests or quizzes, or perhaps in writing assignments in discussion forums.

**Step 6:**
**Recommend the didactic processes that teachers can use**

The final step in the methodology is recommending what didactic processes will be used to convey different elements in the curriculum. Didactic processes are the feedback mechanism that provide students confirmation (or not) of their learning progress. For the instructor, they answer the question: 'how will I teach this material so that students will learn?'

For example, in the stand-and-deliver method of lecturing, the instructor assumes learning is taking place, but may not know until the final exam is given. There are, however, computerized approaches that control the learning process by not allowing students to progress to the next step if they can't pass a quiz on the current one.

Having the material structured through the previous five steps allows the instructor to decide how learning will be assured and the learning process controlled. For our purposes, we discussed various delivery modes as alternatives—guest lectures, conversations with experts. We made decisions about whether to have students break out into discussion groups in class to discuss topics among themselves, or use asynchronous discussion forums monitored online and commented upon by the TA or professor. Alternatively, we decided whether to show videos demonstrating certain hacking concepts or to lead students into a hands-on hacking experience in a guided, air-gapped lab. Didactic processes determine how quickly students learn, how engaged they are and their level of excitement for the subject.

## RESULTS

In the past nine years, applying the KBP model, along with our guiding principles, has resulted in development of 23 individual courses in IA taught in five different disciplines at the University of Washington and the Center's partner schools. In addition several IA certificate programs, degree concentrations and complete degrees either have been launched, or are under construction, with the authors either taking a direct hand in development or acting in an advisory capacity.

Further, one of these programs, the yearlong Information Security and Risk Management (ISRM) Certificate, educated its

**To strengthen our program, we have built an informal alumni organization; many of our graduates come back to lecture and teach in our programs, as well as recruit employees for their respective firms.**

9th cohort in AY2012-13 (Table 2). Growth in the program has been significant. Beginning with 11 students in 2005, last year we graduated 62 successfully. We now conduct two complete cohorts simultaneously—one composed of graduate students, the other of returning adults in continuing education. Of these students, approximately 30% have been women and 13 have been military/veterans from a special outreach program with the Washington National Guard. This program was one of the university's initial offerings through Coursera, with over 24,000 students in the first class. It has been repeated each quarter since. Our retention rates are higher than average and we estimate a total of 50,000 students have completed our series.

The growth of our program may be partially attributable to the reputation of our graduates. Several local firms annually seek opportunities to interview and hire our students. Anecdotally, we know we have had many go into IA careers with industry and government and progress to higher ranks. They are malware and risk analysts, IA auditors, and IA executives and managers. Chief among them are (1) the NCC Deputy Manager, National Communications System, Cybersecurity and Communications within the US Department of Homeland Security, (2) a Technical Director with the National Security Agency, (3) a Chief Information Security Officer with a university in Southern California, (4) CEO and Founder of an IA consulting firm, now in its 4th year, and (5) a senior malware consultant in Washington, DC.

**TABLE 2: ISRM CERTIFICATE GRADUATES 2005-2013**

| Cohort | Academic Year | Total Certificate Students (No. of female) | Total Matriculated Students (No. of female) *[No. of Washington National Guard]* |
|---|---|---|---|
| I | 2005 | 11 | |
| II | 2005-6 | 16 (5) | |
| III | 2006-7 | 18 | |
| IV | 2007-8 | 19 (4) | 16 (4) |
| V | 2008-9 | 17 (5) | 8 (3) |
| VI | 2009-10 | 12 (4) | 14 (4) |
| VII | 2010-11 | 22 (5) | 30 (8) [5] |
| VIII | 2011-12 | 27 (5) | 33 (12) [6] |
| IX | 2012-13 | 28 (6) | 34 (18) [2] |
| **Total** | | **170 (34)** | **135 (49) [13]** |

To strengthen our program, we have built an informal alumni organization; many of our graduates come back to lecture and teach in our programs, as well as recruit employees for their respective firms. We are in the process of formalizing this group and hope to collect additional data regarding career progression of those who have graduated. This will give us more insight into any progress we have made in better preparing students to become IA professionals. Our future work involves continuing to improve our pedagogical processes and assessing our programs against our stated goals.

While the first instantiation of any IAC model requires an investment of time, it has been our experience that it pays off by providing materials that can be leveraged easily to create different instantiations and updated curriculum that keeps pace with change. **Ir**


**References**

[1] Bespalko, V. *Fundamentals of Theory of Pedagogical Systems.* (Vorenege, RU: Voronege State University Press, 1977).

[2] Bloom, B., Mesia, B. and Krathwohl, D. *Taxonomy of Educational Objectives.* (New York: David McKay Company, 1964).

[3] Chabrow, E. "Placing in Context the Infosec Skills Gap: NASCIO's Chad Grant Analyzes Challenges." *GovInfoSecurity.com*, Princeton, NJ. http://www.govinfosecurity.com/interviews/placing-in-context-infosec-skills-gap-i-986. Accessed 2013 June 30.

[4] Chief Information Officer, US Department of Defense. "Information Assurance Scholarship Program: Are You Ready?" *US Department of Defense*, Washington, D.C. http://dodcio.defense.gov/Home/Initiatives/InformationAssuranceScholarshipProgram(IASP).aspx. Accessed 2013 June 30.

[5] Endicott-Popovsky, B., Frincke, D., Popovsky, V. "Designing a Computer Forensics Course for an Information Assurance Track." in *Proceedings of the Eighth Colloquium for Information Systems Security Education.* (West Point, NY: Colloquium for Information Systems Security Education, 2004): 59-64.

[6] Endicott-Popovsky, B., Frincke, D., Popovsky, V. "Secure Code: The Capstone Class in an IA Track." in *Proceedings of the Ninth Colloquium for Information Systems Security Education.* (Atlanta, GA: Colloquium for Information Systems Security Education, 2005).The Printing House, Inc., Stoughton, WI.: 100-108.

[7] Endicott-Popovsky, B., Seifert, C. Frincke, D. "Adopting Extreme Programming on a Graduate Student Project." in *Proceedings of the Sixth IEEE Systems, Man and Cybernetics Information Assurance and Security Workshop.* (West Point, NY: 2005) IEEE Publishing, Los Alamitos, CA. ©2005: 454-455.

[8] Fitzpatrick, A. "For Job Security, Try Cybersecurity, Experts Say." *Mashable.com*, Mashable, Inc., New York. http://mashable.com/2012/05/29/cybersecurity-career/ . Accessed 2013 June 30.

[9] Gates, W. "Trustworthy Computing." *January 15, 2002 Memo.* Microsoft Corporation, Seattle, WA.

[10] Goldman, A. (2009). "Feds Need 10,000 Cyber Security Experts." *Internet News.com*, Quin-Street Enterprise, Louisville, KY. http://www.internetnews.com/security/article.php/3823806. Accessed 2013 June 30.

[11] Hansel, L., Chung, S. and Endicott-Popovsky, B. "Software Reengineering Approach to Teaching Secure Coding Practices. in *Proceedings of the Fifteenth Colloquium for Information Systems Security Education.* (Fairborn, OH: Colloquium for Information Systems Security Education, 2011). The Printing House, Inc., Stoughton, WI: 29-36.

[12] Kuzmina, U. *Fundamentals of Pedagogy of Higher Education.* (Leningrad, RU: Lenizdat, 1972).

[13] Michailova, A. "Establishing a System of Professional–Practical Activity." *Messenger of Higher Education*, Moscow, RU, 11, (1985): 31-33.

[14] National Academies of Science. *Rising above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future.* (Washington, D.C.: The National Academies Press, 2005).

[15] National Security Agency Central Security Service. "National Centers of Academic Excellence." National Security Agency, Washington, D.C. http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml. Accessed 2013 June 30.

[16] NIST/NICE framework. http://csrc.nist.gov/nice/framework/. Accessed 2014 January 6.

[17] Pecinovsky, E. "A Human Capital Crisis in Cybersecurity." *ClearanceJobs.com.* Dice, Inc., Urbandale, IA; http://www.clearancejobs.com/cleared-news/152/a-human-capital-crisis-in-cybersecurity. Accessed 2013 June 30.

[18] Popovsky, V. and Endicott-Popovsky, B. "Integrating Academics, the Community and Industry." in *Proceedings of the Physical Culture and Sports: Analysis of Social Processes '08.* (St. Petersburg, RU: 2008), Lesgaft National State University Press, St. Petersburg, RU: 239-243.

[19] Popovsky, V. "Coaching Volleyball with Unleashing Personal Potential in Mind." in *Proceedings of the Int'l Conference Honoring 70th Anniversary Sports Games Dept. Lesgaft State Academy of Physical Education '04*, (St. Petersburg, RU 2004), Lesgaft National State University Press, St. Petersburg, RU: 136-140.

[20] Popovsky, V., Endicott-Popovsky, B., "Physical Culture Pedagogy: Coaching by Design." in *Methods for Modernizing Physical Culture: Selection of Scientific and Methodological Works*, edited by V.E. Grigoriev, (St. Petersburg, Russia, 2005): 176-187.

cybersecurity education

## Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals

[21] Roginsky, V. *Alphabet of Pedagogical Work*. (Moscow, RU: Higher Education, 1990).
[22] Simpson, J. and Endicott-Popovsky, B. "A Systematic Approach to Information Systems Security Education." in *Proceedings of the Fourteenth Colloquium for Information Systems Security Education*, (Baltimore, MD: Colloquium for Information Systems Security Education, 2010). The Printing House Inc., Stoughton, WI: 173-179.
[23] Simpson, J., et al. Secure software education: A contextual model-based approach. *International Journal of Secure Software Engineering*, (2010). 1(4). pp. 35-61.
[24] Talizina, N. Activity approach to the development of the model specialist. Messenger of Higher Education, Moscow, RU, 11, (1986): 10-13.
[25] Talizina, N. *Management of the Learning Process*. (Moscow, RU. Higher Education, 1975).
[26] US Office of Personnel Management. "Cybercorps: Scholarship for Service." https://www.sfs.opm.gov/. Accessed 2013 June 30.
[27] Wiggins, G. and McTighe, J. *Understanding by Design*, 2nd ed. (Alexandria, VA: Association for Supervision and Curriculum Development, 2005).

**BARBARA E. ENDICOTT-POPOVSKY**
University of Washington
Information School
4311 11th Avenue NE, Suite 400
Seattle, Washington 98105 USA
*endicott@uw.edu*

**VIATCHESLAV M. POPOVSKY**
University of Idaho
HERD
709 South Deakin Street
Moscow, Idaho 83844 USA
*dr_popovsky@hotmail.com*

**Categories and Subject Descriptors:** K.3.2
**General Terms:** Security
**Keywords:** cybersecurity, education and workforce development, pedagogy

**DOI:** 10.1145/2568195.2568214 