CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

What Business Leaders Can Expect from Security Degree Programs

Key Message: Information security degree programs are proliferating – but what do they really offer business leaders who are seeking knowledgeable employees?

Executive Summary

As information security continues to evolve from ad hoc art to specialized science, more and more academic institutions are launching undergraduate and graduate degree programs that focus on this fast-growing field.

In this podcast, Sean Beggs, program director of Carnegie Mellon's Master of Science in Information Security Policy & Management, discusses what employers can expect from graduates of information security programs, what students in those programs are seeking in an employer, and how employers can help ensure newly hired graduates will succeed.

PART 1: NUTS AND BOLTS VERSUS THE BIG PICTURE

A Focus on Process

The **process** by which to attack information security problems is one of the most important skills a student in an information security program can acquire.

Process means the underlying factors found within, around, or resulting from information security issues.

Process isn't the messy details of configuring a router. Although that's important on some level, the big picture is far more vital.

Complementing Students' Existing Knowledge

Undergraduate and graduate programs often may differ. For example, undergraduate programs may be more focused on building foundational skills, while graduate programs may focus on skills needed to perform as a senior security professional.

Even within each type of framework, students' backgrounds may differ. One worthwhile goal may be to reach across disciplines and give each student what he or she doesn't have.

So, if an incoming student is technology-savvy and, for example, can configure a router already, the degree program ideally should help that student appreciate the other, more abstract aspects of information security.

Meanwhile, if another incoming student doesn't know what a router is beyond its use in a home office, the degree program ideally should help the student appreciate what routers are capable of from a security standpoint.

Finding the Balance

The end goal is really to bridge all of the various disciplines that play a role in information security, and to produce graduates who can oversee the entire security life cycle and evolution of an infrastructure, including:

- planning
- acquisition

- development
- evolution

It is a balance between a reliance on nuts-and-bolts security practices and technologies, and a reliance on policy. The intersection between those two areas is compelling. Someone who bridges both can focus on the big picture while keeping in mind technology considerations.

PART 2: HOW TO HELP ENSURE GRADUATES ARE SUCCESSFUL

Identifying and Recruiting Candidates

How can a business leader identify programs that are teaching the kinds of skills they need in their organization?

One source is the National Security Agency's Centers of Academic Excellence in Information Assurance Education.

And what are students looking for in an employer?

One main characteristic (besides a good salary!) may be **support** – or, more specifically, employers that make active investments in their security personnel, encouraging them to learn more through, for example, pursuing certification and attending security conferences.

Gauging Students' Knowledge

What are some good questions that could help interviewers gauge students' level of preparedness for real-world work?

Ask how a student:

- Thinks about information security
- Mentally calculates and identifies all of the angles involved in an information security problem

The student's answer will tell you something about:

- What the individual is like
- How the individual will tackle an ever-changing security landscape

This approach can really tease out more than a list of courses taken will tell you. The list of courses tell you what a student is supposed to know, but asking the right questions tell you how much they really know and how they will apply it.

This approach helps ensure the right fit with the organization and its culture.

Smoothing the Transition Path

After making a hiring decision, organizations can take steps to ensure new graduates have a successful transition to the work world.

For example, a 100-day plan could be very helpful, defining:

- The organization's expectations of the graduate
- The chain of command within the organization
- A statement of how things get done within the organization
- How all associates fit together within the organization to achieve the organization's goals

Why Security Programs?

Why hire a graduate of a security program, rather than someone from a computer science program who is more self-taught in security?

- It's difficult to measure the skill level of a self-taught individual, in some cases.
- A degree indicates a person has achieved certain measurable standards, which can be a benefit for an organization that wants to market certain expertise to its customers.
- A degree shows specific commitment to the field of information security.

PART 3: KEEPING PACE AS THE SECURITY FIELD EVOLVES

Planning for the Future

A couple of things may happen as the information security field evolves.

In one scenario, information security becomes almost second nature, like using a telephone. However, this seems unlikely.

In the other scenario, the issues will simply change. As one problem is fixed, another will arise. There will always be people asking, "How can I break this? How can I beat the system?" And there will always be a need for people to defend against the issues and exploits that result.

It is possible that information security may evolve to a point of increasing specialization. But it's difficult to say if this will happen; in many ways, the future evolution of the field will be shaped by the people being trained today.

Influencing Course Requirements

In such a fluid environment, the process of choosing what to teach and what not to teach in an information security program is driven by three things:

- The academic institution's organizational objectives (research versus for-profit)
- The types of organizations where program graduates go to work
- The types of tasks new graduates of the information security program are asked to do by their employers

A formal feedback process from employers to academic institutions likely would be helpful in this process as well, but it does not exist right now.

Resources

Carnegie Mellon MSISPM program

Software Engineering Institute