November 2019

LONGWOOD UNIVERSITY

INFORMATION SECURITY

Preparing Students for the Cybersecurity Job Market

Behind every new report of a data breach, data leak, or computer hack is a company scrambling to put out the fire, which is great news for job seekers or soon-to-graduate students with cybersecurity skills. Unfortunately, this is bad news for most companies because there is currently an imbalance between the supply and demand of skilled professionals to address these vulnerabilities.

The 2018 $(ISC)^2$ Cybersecurity Workforce Study estimates a global shortage of cybersecurity professionals of around three million workers. This shortage of skilled job seekers is having a real-world impact on companies and the people responsible for cybersecurity at those companies. The study also points out that Gen X and Baby Boomer workers make up about half of the current cybersecurity workforce, leaving many entry-level opportunities for new college graduates and pathways for growth as these more experienced workers approach retirement age.

The need for trained cybersecurity professionals is not going to go away. The US Bureau of Labor Statistics projects a 28% growth in US employment for cybersecurity consultants between 2016 and 2026. How can we help our students go beyond the theoretical concepts taught in computer science or cybersecurity classes and make themselves more attractive to future employers? We need to take the lead to encourage students to take the initiative to learn more about current issues in cybersecurity and take advantage of the many cybersecurity resources available.

Here are some ways you can help your students and contribute to narrowing the cybersecurity skills gap:

Continued on page 3

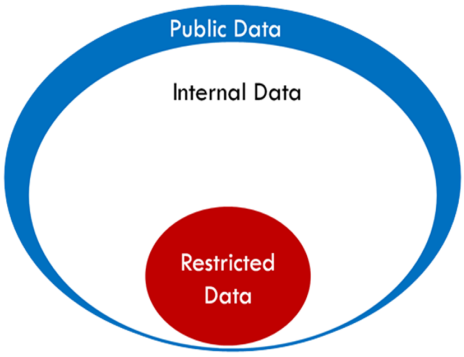
Inside this issue

Data Classification..... 2
Working with Vendors..... 2
Preparing Students, Con't..... 3
Online Shopping Tips 4

Special points of interest

- Additional access may require additional training in Securing the Human; be prepared to finish new modules as they're assigned.
- Keep your eyes out for changes to our security training next year!

Data Classification



If you deal with data at Longwood, it's important to understand how that data is classified. Our data is classified according to its **sensitivity**, or the likelihood that the data will compromise the three principles of security: confidentiality, integrity, and availability. We have three categories of data:

- **Public Data:** The least sensitive information, suitable for public consumption. This is the kind of data that you might see on our website or in a press release.
- **Internal Data:** Moderately sensitive information that we want to keep within the university. Examples of internal data would include meeting minutes or project documents. Student data is internal data that is protected under the Family Educational Rights and Privacy Act (FERPA). See the Registar's Office for information about FERPA data.
- **Restricted Data:** Highly sensitive information for which an unauthorized disclosure may result in identity theft or university liability for costs or damages under laws, government regulations or contract.

If you deal with restricted data, contact the Information Security office at infosec@longwood.edu to receive special training for handling it.

Did You Know?

- The project management office provides guidance, support, and oversight for Longwood University ITS projects.
- We assist university departments in exploring and deploying ITS solutions to a broad spectrum of academic and administrative needs.
- If you need assistance with a project, please call the Project Management Office at 434-395-2896 or email help@longwood.edu.

Working with Vendors

Getting ready to send data to a vendor or sign a contract? With more and more services moving to the cloud, Longwood has an additional obligation to ensure that third parties are protecting our most sensitive information. If you or your department is looking to purchase or adopt a service or technology that uses institutional data, it is imperative that you include the Project Management Office of Information Technology Services (ITS) at the beginning of the project or contract process to help ensure that data are properly protected. To determine whether or not ITS should be involved in the vendor/contract process, ask yourself the following questions:

- Does the project (and in-scope technologies) involve the handling or storage of personal data (e.g., student data, employee data, donor data, research data, or financial data)?
- Does the project (and in-scope technologies) involve the handling or storage of personal data that is regulated by government entities or has special contractual obligations to a third party (e.g., contract sponsored for research)?
- Is there transfer of any institutional data from an institution-owned system or device to a third-party vendor-contracted system or device?
- Does the project involve acquiring/implementing/developing software, services, or components that your institution has not previously deployed?
- Does the project involve providing a new data feed to an existing campus partner?
- Does the project involve accepting card payments in any way?

If the answer to any of the above questions is "yes," collaborate with the Project Management Office at the beginning of the project to ensure that institutional data are properly protected.

Preparing Students, Con't.

Hold informational sessions on cybersecurity. Help spread the word on your campus about the cybersecurity skills gap and job opportunities. You could ask your CIO or information security team to conduct a cybersecurity seminar or invite local experts to share their knowledge and expertise with your students. The Enterprise Security Team at The Ohio State University has already implemented this idea, and they sponsor an annual and free on-campus Cybersecurity Days event to expand knowledge of security and data protection for their entire college community.

Sponsor or encourage membership in student associations. There are two student cybersecurity organizations for your students to explore—National Cybersecurity Student Association and Women in CyberSecurity (WiCyS). The National Cybersecurity Student Association has a number of resources on their website, and you can sign up for their newsletter or follow their Snapchat account to view a day in the life of a cyber student or industry professional. The WiCyS is dedicated to bringing together women in cybersecurity from academia, research, and industry to share knowledge, experience, networking, and mentoring. You can also explore setting up a local WiCyS student chapter on your campus.

Offer campus internships. In addition to knowledge of advanced cybersecurity concepts, the most important qualification for cybersecurity employment is relevant work experience. The Information Security office can hire students as interns. This offers students real-world experience while providing supplemental staffing for the department. For suggested qualifications and responsibilities, use the Information Security Intern Job Description Template on the EDUCAUSE website as a starting point.

Identify scholarship opportunities. The CyberCorps: Scholarship for Services, funded by the NSF, provides up to $22,500 per year for undergraduates and $34,000 per year for graduate students. In return, students commit to work for a federal, state, or local agency for a period matching the length of their scholarship. The Cyber Security Degree website provides a comprehensive list of additional cybersecurity scholarships and other career resources.

Encourage students to deepen their knowledge. The NICCS Education and Training Catalog is a central location where cybersecurity professionals across the nation can find more than 3,000 cybersecurity-related courses. Anyone can use the interactive map and filters to search for courses offered in their local area to add to their skill set, increase their level of expertise, or earn a certification. You could also direct your students to take advantage of the free online courses offered through edX, US Department of Homeland Security, Cybrary, or SANS Cyber Aces Online.

Attend cyber competitions. Institutions with an information assurance or computer security curriculum can give their students an additional way to hone their skills and have fun by participating in regional events hosted by the National Collegiate Cyber Defense Competition (NCCDC). The top regional teams can then go on to the National Championship, which was won by University of Virginia in 2018. Another cybersecurity competition for high school and college students is the National Cyber League (NCL), a defensive and offensive puzzle-based, capture-the-flag style competition. All participants play the games simultaneously and are tested with real cybersecurity challenges they will likely face in the workforce.

Participate in cybersecurity conferences. Students may be interested in the educational and networking opportunities from attending the annual conferences for the National Cybersecurity Student Association or Women in CyberSecurity. For additional conferences in your area, InfoSec publishes a comprehensive list with hundreds of cybersecurity events in the United States, Europe, and Asia.

Resources

- Use the free National Cyber Security Alliance Cyber Career Paths infographic.
- View and download the NCSA's Securing Our Future: Closing the Cyber Talent Gap infographic.
- Find out how you can participate in the Collegiate Cyber Defense Competition (CCDC) or the National Cyber League (NCL).
- Learn about the CyberCorps: Scholarship For Service.
- Explore the Department of Homeland Security (DHS) Cybersecurity Workforce Development Toolkit and Cybersecurity Workforce Portal.
- Read the $(ISC)^2$ article on Starting Your Cybersecurity Career.
- Check out the National Cybersecurity Workforce Framework (a.k.a., the *NICE Framework*).
- Browse the National Initiative for Cybersecurity Careers and Studies (NICCS) Training Catalog or view the NICCS informational video.

Online Shopping Tips

The Office of Information Security is responsible for developing and implementing campus-wide policies, controls and procedures to protect the university's information technology resources and systems from intentional or inadvertent modification, disclosure or destruction, as well as monitoring user adherence to these policies.

The holidays are coming, and many people will be shopping online to avoid crowds and to find that perfect gift. Keep these tips in mind when you shop online:

- **Conduct Research:** When using a new website for purchases, read reviews and see if other consumers have had a positive or negative experience with the website.
- **Clean It Up:** Links in emails, posts and texts are often the ways cybercriminals try to steal your information or infect your devices.
- **Protect Your Information:** When making a purchase online, be alert to the kinds of information being collected to complete the transaction. Make sure you think it is necessary for the vendor to request that information. Remember, you only need to fill out required fields at checkout.

These tips are on a tip sheet from a Stop. Think. Connect. Check them out at staysafeonline.org.

Longwood University

Information Technology Services
French Hall
201 High Street
Farmville, VA 23909
(434) 395-4357
(434) 395-2034

Fax: (434) 395-2035