KEEPING OUR PERSONAL HEALTH INFORMATION SAFE

THANKS TO A STEADY RISE OF DATA BREACHES IN HEALTH CARE, THERE'S A GROWING NEED FOR CYBERSECURITY PROFESSIONALS WITH THE TARGETED KNOWLEDGE AND SKILLS TO PROTECT OUR PERSONAL HEALTH INFORMATION.

CAPELLA UNIVERSITY'S MASTER OF SCIENCE IN INFORMATION ASSURANCE AND CYBERSECURITY, HEALTH CARE SECURITY SPECIALIZATION IS ALIGNED WITH INDUSTRY STANDARDS TO PREPARE PROFESSIONALS TO BUILD THE SECURITY INFRASTRUCTURE THAT SERVES THIS IMPORTANT AND GROWING NEED.

INFORMATION SECURITY
CAREER CENTRAL

Powered by Capella University

SUMMARY

PERSONAL HEALTH INFORMATION (PHI) IS HIGHLY VALUABLE TO CYBERCRIMINALS DUE TO THE TROVE OF SENSITIVE INFORMATION INCLUDED IN OUR HEALTH RECORDS: SOCIAL SECURITY NUMBERS, DATES OF BIRTH, MEDICAL HISTORY, INSURANCE INFORMATION, AND OTHER VALUABLE DATA USED TO IDENTIFY PATIENTS, DETERMINE CARE, AND SECURE PAYMENTS FOR SERVICES.

Cybersecurity professionals with the specialized skills and knowledge to protect health care systems from unauthorized access, theft, and hacking are in high demand. Capella's Master of Science in Information Assurance and Cybersecurity, Health Care Security Specialization provides the foundational knowledge and hands-on experience required to meet these challenges.

Capella University has been designated by the National Security Agency (NSA) and the Department of Homeland Security (DHS) as a National Center of Academic Excellence in Information Assurance/Cyber Defense (CAE IA/CD) for academic years 2014–2021.

CHALLENGE

HEALTH CARE INFORMATION IN JEOPARDY

As health care and insurance providers work to meet regulatory requirements and offer greater accessibility and convenience to their patients, highly sophisticated criminals are focused on leveraging vulnerabilities to gain access to personal health information (PHI).

Stolen PHI can be used to procure medical devices or prescription drugs, file false insurance claims, commit Medicare fraud, and blackmail patients and providers. Unlike financial information, which is only valuable until the theft is noticed and the account is canceled, PHI has a long shelf life. This, coupled with the fact that multiple data points are included in PHI, has driven up its value.

HEALTH CARE DATA RISKS AND COSTS CONTINUE TO RISE:

- CRIMINAL ATTACKS ON HEALTH CARE DATA GREW 125 PERCENT FROM 2010 TO 2015.[1]
- BETWEEN 2015 AND 2019 APPROXIMATELY ONE IN 13 PATIENTS—MORE THAN 25 MILLION PEOPLE—WILL HAVE THEIR MEDICAL AND/OR PERSONAL INFORMATION STOLEN AS A RESULT OF A CYBERATTACK.[2]
- MEDICAL RECORDS HAVE BEEN ESTIMATED TO BE WORTH 10 TO 20 TIMES THAT OF FINANCIAL DATA.[3]
- THE AVERAGE COST OF A DATA BREACH FOR HEALTH CARE ORGANIZATIONS IS $2.1 MILLION.[4]
- PATIENTS WHO ARE VICTIMIZED WILL SPEND AN ESTIMATED $13,500 AND 200 HOURS TO ADDRESS THE CONSEQUENCES OF MEDICAL IDENTITY THEFT.[5]

THE INDUSTRY SCRAMBLES TO PROTECT DATA

Although health care organizations are prioritizing information security to protect systems and quickly detect data breaches, many are struggling to address current vulnerabilities. In particular, hiring professionals with the specialized health care security skills required to keep PHI safe is proving to be a challenge.

ONLY 53%

OF HEALTH CARE ORGANIZATION REPRESENTATIVES AGREE THAT PERSONNEL HAVE THE TECHNICAL EXPERTISE TO IDENTIFY AND RESOLVE DATA BREACHES INVOLVING THE UNAUTHORIZED ACCESS, LOSS OR THEFT OF PATIENT DATA.[6]

ONE-THIRD OF SURVEYED HEALTHCARE IT EXECUTIVES REPORTED A PROJECT ON HOLD BECAUSE OF IT VACANCIES.[7]

[1]SOURCE: Ponemon Institute. Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data. http://www.ponemon.org/blog/criminal-attacks-the-new-leading-cause-of-data-breach-in-healthcare

[2]SOURCE: Accenture. The $300 Billion Attack: The Revenue Risk and Human Impact of Healthcare Provider Cyber Security Inaction. https://www.accenture.com/t20150723T115443__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_19/Accenture-Provider-Cyber-Security-The-$300-Billion-Attack.pdf

[3]SOURCE: Insurance Journal. Healthcare Firms at Risk; Hackers Value Medical Records Over Credit Data. http://www.insurancejournal.com/news/national/2014/09/26/341691.htm

[4]SOURCE: Ponemon Institute.

[5]SOURCE: Ponemon Institute.

[6]SOURCE: Ponemon Institute.

[7]SOURCE: HIMSS. 2014 HIMSS WORKFORCE STUDY. http://www.fastswitch.com/menu_assets/images/2014_HIMSS_Workforce_Survey.pdf

SOLUTION

BUILDING A WORKFORCE OF SKILLED HEALTH CARE SECURITY PROFESSIONALS

Just as a team of doctors, nurses, and care coordinators is often required to address health care challenges, securing our PHI requires the efforts of many cybersecurity professionals working toward a common goal. Health care security teams can include:

- **Health Information Manager:** Maintains and secures patient records. Ensures complete, accessible, and accurate data is available to inform patient care, research, and quality controls. Ensures only authorized personnel have access to information.
- **Compliance Officer:** Follows governmental guidelines to develop, implement, and monitor compliance program. Responsible for internal audits, risk assessment, and compliance reviews, as well as staff education and training.
- **Information Technology Manager:** Responsible for purchasing, modifying, developing, and securing software applications to manage administrative processes, including billing, payments, and insurance filings.
- **Information Security Manager:** Responsible for ongoing availability, confidentiality, and integrity of employee, patient, provider, and business information. Follows organizational security policies as well as governmental regulations.
- **Risk Analyst:** Develops, coordinates, and administers systems for risk identification, reduction, and analysis. Typically reports to leadership on risk management status, issues, and resolutions.

THE RIGHT OF EDUCATION

According to research firm Burning Glass, 23 percent of cybersecurity job postings require a master's degree. To develop the skills and knowledge needed to fill these positions, working professionals need targeted health care security master's degree programs that are:

- **Practical,** featuring hands-on learning experiences
- **Tailored** to improve targeted competencies
- **Flexible** and convenient for working professionals
- **Aligned** to provide immediate on-the-job impact
- **Supportive** of preparation for relevant certifications
- **Marketable** in today's health care security sector

Certifications are another way to verify specific knowledge and abilities. In addition to the more general and highly respected Certified Information Systems Security Professional (CISSP®) from (ISC)[2], certifications that focus specifically on health care security are highly respected in the job market:

- **Information Security and Privacy Practitioner (HCISPP®)** from (ISC)[2]
- **Certified in Healthcare Privacy and Security (CHPS®)** from AHIMA

[8]SOURCE: Burning Glass. Burning Glass Report on Cybersecurity Jobs. http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

RESULTS

CAPELLA'S MASTER OF SCIENCE IN INFORMATION ASSURANCE AND CYBERSECURITY, HEALTH CARE SECURITY SPECIALIZATION

Capella University has answered the call for a high-quality master's program that delivers the skills and knowledge required to protect our PHI.

Capella's Master of Science in Information Assurance and Cybersecurity, Health Care Security specialization is professionally aligned and delivered by faculty with practical and academic experience in health care cybersecurity, preparing students to:

- Implement physical and technical information safeguards in the health care environment
- Develop and apply investigative, compliance, and enforcement processes
- Develop best practices for information management of vital health care data
- Analyze ethical, legal, and regulatory issues related to health care security, privacy, and compliance

Capella programs are designed to meet the needs of working adults. With online classes that are aligned with professional standards and available anywhere and anytime, busy professionals can gain the skills required for career success at a time and place that fits their schedule.

HANDS-ON LEARNING

Students in Capella's MS in Information Assurance and Cybersecurity, Health Care Security specialization will practice their skills in a secure virtual lab that provides hands-on experience with the industry-specific tools that health care employers require.

CERTIFICATION EXAM PREPARATION

The curriculum is designed around industry standards, so in addition to providing the right skills to meet industry needs, this master's program helps students earn relevant, industry-specific certifications.

The foundational knowledge covered in this degree prepares students for the HealthCare Information Security and Privacy Practitioner (HCISPP®) and Certified in Healthcare Privacy and Security (CHPS®) exams. Additionally, the core curriculum in this program includes a common body of knowledge represented in several leading security certifications, including the CISSP®.

ABOUT CAPELLA

Capella University is an accredited online university. Capella offers graduate and undergraduate specializations as well as certificate programs designed to help working adults advance in their careers.

NATIONAL SECURITY AGENCY DESIGNATION

Capella University has been designated by the National Security Agency (NSA) and the Department of Homeland Security (DHS) as a National Center of Academic Excellence in Information Assurance/Cyber Defense (CAE IA/CD) for academic years 2014–2021.

EXCEPTIONAL FACULTY

Most of Capella's faculty in the School of Business and Technology hold doctorates. They also bring real-world expertise to the courseroom, with many holding current positions in small businesses, government, non-profits, consulting, and higher education. Many faculty members are published authors and industry leaders at organizations such as IBM, Microsoft, and Vulcan Systems.