CYAI
Cybersecurity
Youth Apprenticeship Initiative

The Importance of Cybersecurity in Every Industry

June 2022

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.

Cybersecurity in Every Industry

Cybersecurity impacts businesses at every level and can quickly jeopardize business operations.[1] From the risk of exposure of sensitive client information to the risk of stalled production times or halted medical services, there are multiple ways through which a bad actor could destabilize an organization's function and reputation. Many businesses are susceptible to cyberattacks because they lack sufficient security measures, or they simply do not have adequate cybersecurity professionals employed to help them. Businesses must recognize the importance of a robust cybersecurity protocol to protect the data and information that they collect and store.

The cost of preventing cyberattacks is cheaper than the cost of recovery from an attack.[2] As many as sixty percent of businesses fail within six months of being targeted by bad actors.[3] This white paper highlights the importance of cybersecurity within different industries. It then demonstrates how registered apprenticeship can attract and retain talent to cybersecurity jobs to address this overwhelming business need.

Government

Over the past nine years, the number of cyberattacks that government agencies experienced grew from 5,000 attacks per year to 77,000 in one year.[4] Government agencies host personal information about residents as well as financial data and information related to national security. Much of this data is collected and stored electronically, making the hosting systems an attractive option for bad actors to breach and expose sensitive security and civilian information. There are many public and private systems that are vital to the Nation's security and dependent on IT systems to carry out day-to-day operations, including energy, transportation, communications, and financial services.[5] Cyberattacks can impact the daily workings of these systems and cause critical harm to government operations and public safety. Both public and private systems operate on electricity grids and telecommunication systems that can be disrupted if not properly protected.[6] These weaknesses within the

2021 Threat to US Water Treatment Facility

In February 2021, CISA issued an alert explaining that cyber threat actors obtained unauthorized access to a U.S. water treatment facility's industrial controls systems and attempted to increase the amount of a chemical that is used as part of the water treatment process. CISA reported that the actors were likely able to obtain access due to the facility's weak password protection and an outdated operating system.

CISA, Compromise of U.S. Water Treatment Facility, Alert AA21-042A (Feb. 11, 2021).

[1] CISA. (2021, August 11). *The business case for security*. CISA.gov. Retrieved from https://staysafeonline.org/wp-content/uploads/2017/09/Communicating-with-the-Board-about-Cybersecurity-Making-the-Business-Case.pdf

[2] CISA. (2021, August 11). *The business case for security*. CISA.gov. Retrieved from https://staysafeonline.org/wp-content/uploads/2017/09/Communicating-with-the-Board-about-Cybersecurity-Making-the-Business-Case.pdf

[3] Galvin, J. (2018, May 7). *60 percent of small businesses fold within 6 months of a cyber attack. here's how to protect yourself*. Inc.com. Retrieved from https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html

[4] Western Governors University. (2018, December 7). The Need for Cybersecurity Experts in Government. Western Governors University. Retrieved from https://www.wgu.edu/blog/need-for-cyber-security-experts-government1811.html

[5] U.S. Government Accountability Office, U. S. G. A. O. (2021, April 22). *High-risk series: Federal Government needs to urgently pursue critical actions to address major cybersecurity challenges*. Retrieved from https://www.gao.gov/products/gao-21-288

[6] U.S. Government Accountability Office, U. S. G. A. O. (2021, April 22). *High-risk series: Federal Government needs to urgently pursue critical actions to address major cybersecurity challenges*. Retrieved from https://www.gao.gov/products/gao-21-288

government's infrastructure must be addressed and can be helped by more comprehensive cybersecurity plans and a stronger cyber workforce across all agencies.

Finance

Financial services is one of many industries that collects personally identifiable information (PII) from customers, including addresses, social security numbers, and income details. Because financial service providers such as banks, credit card companies, and investment firms store this PII, they are often targeted by bad actors via ransomware, malware, phishing campaigns, or hacking.[7] Unencrypted data and unprotected mobile applications are two major vulnerabilities for many banks.[8] According to the *Security Cost of a Data Breach* report published by IBM, in 2019, the average cost per breach within financial services was $5.86 million.[9]

Healthcare

Like finance, the healthcare industry collects a plethora of PII, making this industry another attractive target for bad actors. Many healthcare organizations rely on specialized technology such as electronic health record (EHR) systems, e-prescribing systems, practice management support systems, clinical decision support systems, radiology information systems and computerized physician order entry systems to provide comprehensive patient care.[10] According to the IBM Security Data Breach Calculator, the cost to remediate a breach in health care is almost three times that of other industries — averaging $408 per stolen health care record versus $148 per stolen non-health record.[11] Health care providers use devices like smart elevators, heating, ventilation and air conditioning (HVAC) systems, infusion pumps, and remote patient monitoring devices that are reliant on databases and connected to the internet and are thus even more at risk of breaches.[12] Breaches to the technology used by health care providers can impact the safety and health of patients.[13] Patient safety is directly tied to cybersecurity. Cybersecurity professionals are greatly needed in the healthcare industry to

March 2021 CNA Cyberattack
A Chicago based insurance company experienced system shutdowns after a cyberattack exposed the PII of more than 75,000 customers. The ransomware attack disrupted CNA networks and upset their website functionality. CNA paid the hackers $40 million to regain control of its systems.

Channick, R. (2021, November 2). *CNA cyberattack in March exposed personal information of more than 75,000 people, filings reveal.* chicagotribune.com

[7] Bowcut, S. (2021, February 25). Cybersecurity in the Financial Industry. Cybersecurity Guide. Retrieved from https://cybersecurityguide.org/industries/financial/

[8] Romeo, K. (2020). The Importance of Cybersecurity in Banking. Bank Business eMagazine. Retrieved from https://www.bankbusiness.us/the-importance-of-cybersecurity-in-banking/

[9] IBM Security. (2019). 2019 cost of a data breach report - ibm.com. IBM. Retrieved from https://www.ibm.com/downloads/cas/ZBZLY7KL

[10] Epalm. (2021, December 16). Cybersecurity in Healthcare. HIMSS. Retrieved from https://www.himss.org/resources/cybersecurity-healthcare

[11] Ibm. (2018, July 17). Cost of Healthcare Data Breach is $408 per stolen record, 3x Industry Average says IBM and Ponemon I. Healthcare Digital.

[12] Epalm. (2021, December 16). Cybersecurity in Healthcare. HIMSS. Retrieved from https://www.himss.org/resources/cybersecurity-healthcare

[13] Pachucki, W., Krajewski, M., de'Medici, B., Oar, G., Letterman, C., Wassef, H., Clark, J., Littlefield, K., & Kim, L. (2019). *A lifeline: Patient safety and cybersecurity*. Department of Homeland Security. Retrieved from https://www.dhs.gov/sites/default/files/publications/ia/ia_vulnerabilities-healthcare-it-systems.pdf

design systems that safeguard patient data and health care technology, such as improved firewalls, encryption solutions, and segmented networks.[14]

Manufacturing

Manufacturers rely on machinery and tools to produce goods on a mass scale, which makes them vulnerable to cyberattacks.[15] By 2018, 60 percent of heavy industry companies experienced a data breach in their industrial or supervisory control and data-acquisition systems.[16] In recent years, manufacturers have become targets for ransomware attacks, which can halt production and cause sizeable money loss for companies. Manufacturers were crucial to the healthcare supply chain as they increased production of protective equipment for health care professionals during the COVID-19 pandemic.[17] A halt in production disrupts the entire supply chain and impacts consumers.

Online Retail

E-commerce has exploded in scale and scope. Retailers switched to online orders to reach customers across the globe while they're at home or on-the-go.[18] They collect and store PII and financial information to process transactions when customers make purchases. This customer data is usually stored in a cloud database that is an attractive target for bad actors.[19] In a 2020 survey, 34% of retailers said concerns surrounding cybersecurity were their primary challenge with entering into the world of e-commerce.[20] Strategies like the implementation of encryption services and installation of surveillance software can help increase retailer's cybersecurity defenses.[21]

November 2013 Target Hack
The infamous attack on giant retailer Target stole 40 million credit card numbers, and 70 million customer records through an unprotected HVAC system. The breach jeopardized customer loyalty and brand reputation and cost the company millions.

Retrieved from https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

[14] Norwich University Online. (2020, April 20). The Role of Cybersecurity in Healthcare and Hospitals. Norwich University Online. Retrieved from https://online.norwich.edu/academic-programs/resources/cybersecurity-in-healthcare

[15] Khemani, R. (2021, April 13). Cyber Security for manufacturing firms: 5 reasons & 5 ways. Security Boulevard. Retrieved from https://securityboulevard.com/2021/04/cyber-security-for-manufacturing-firms-5-reasons-5-ways/

[16] Booth, A., Dhingra, A., Heiligtag, S., Nayfeh, M., & Wallance, D. (2021, October 12). Critical Infrastructure Companies and the Global Cybersecurity Threat. McKinsey & Company.

[17] Kessem, L. (2021, March 31). Threat actors' most targeted industries in 2020: Finance, manufacturing, and Energy. Security Intelligence. Retrieved from https://securityintelligence.com/posts/threat-actors-targeted-industries-2020-finance-manufacturing-energy/

[18] Bisson, D. (2021, March 4). The shift to e-commerce: How retail cybersecurity is changing. Security Intelligence. Retrieved from https://securityintelligence.com/articles/shift-e-commerce-how-retail-cybersecurity-is-changing/

[19] Gregory, J. (2021, March 15). Retail Cybersecurity: How to Protect Your Customer Data. Security Intelligence. Retrieved from https://securityintelligence.com/articles/retail-cybersecurity-how-to-protect-your-customer-data

[20] BDO USA, LLP. (2020). 2020 Technology Digital Transformation Survey. BDO. Retrieved from https://www.bdo.com/getmedia/c03ae511-54c8-4229-bc0e-017414055b0b/ADV_DTS_Middle-Market-DTS_Tech_Web_Final.pdf

[21] Gregory, J. (2021, March 15). Retail Cybersecurity: How to Protect Your Customer Data. Security Intelligence. Retrieved from https://securityintelligence.com/articles/retail-cybersecurity-how-to-protect-your-customer-data/

Marketing and Communications

Marketing campaigns drive the relationship between businesses and their clients. Digital marketing and social media are an efficient way for businesses and their operations to reach their existing and target customers. Firms collect and analyze consumer data and online behavior to tailor their marketing strategies.[22] However, storing and protecting this personal information is essential. One breach of data or hacked social media account can jeopardize consumer trust in a brand. Initiating security audits of databases and working with IT security software experts is a key step in keeping business information safe.

How Apprenticeship can Solve the Cybersecurity Workforce Gap

There is a clear need for cybersecurity talent in every industry. One proven, successful strategy to recruit, train, and retain talent is through a registered apprenticeship program (RAP). RAPs integrate on-the-job training and classroom learning to provide apprentices with a supported "earn while you learn" job experience. Apprentices receive a clearly defined amount of classroom instruction that is applied on the job under the tutelage of a company mentor. The apprentice is paid to succeed at a graduating rate and with goals set by the employer. When they complete the apprenticeship, they are skilled and work-ready by the employer's specifications.

Table 1 provides an overview of entry level cybersecurity roles as well as their associated titles and requested skills. Entry level roles in cybersecurity function as a springboard for a registered apprenticeship program.

Table 1: Entry Level Cybersecurity Roles and Associated Titles[23]

Role	Associated Position Titles	Skills Requested
Cybersecurity Specialist	• Security Specialist • Information Security Specialist • Cyber Security Specialist • IT Security Specialist • IT Specialist Information Security	• Information Security • Information Systems • Information Assurance • Network Security • Security Operations • Vulnerability assessment • Project Management • Linux
Cyber Crime Analyst	• Digital Forensics Analyst • Digital Forensic Examiner • Cyber Security Forensic Analyst • Cyber Forensic Specialist • Computer Forensics Analyst	• Information Security • Security Operations • Cryptography

[22] Chambers, B. (2021, July 30). Why Marketers Should Care About Cybersecurity. Forbes. Retrieved from https://www.forbes.com/sites/forbescommunicationscouncil/2021/07/30/why-marketers-should-care-about-cybersecurity/?sh=3e85c503c972

[23] Cyberseek. (2020). Cybersecurity Career Pathway. Retrieved from https://www.cyberseek.org/pathway.html

Role	Associated Position Titles	Skills Requested
Incident & Intrusion Analyst	• Senior Analyst, Information Security • IT Security Project Manager • Network Technical Specialist • Disaster Recovery Specialist • Audit Project Manager - Information Security	• Information Security • Security Operations • Cryptography • Risk Assessment & Management • Threat Analysis • Authentication • Network Security
IT Auditor	• IT Auditor • IT Audit Manager • Internal IT Auditor • IT Audit Consultant • Information Technology Manager	• Information Security • Security Operations • Risk Assessment & Management • Threat Analysis • Authentication • NIST Cybersecurity Framework • Internal Auditing

With a half million open cybersecurity positions, there is just too much at stake and too much competition for talent for employers to risk playing the talent lottery. Apprenticeships are a proven method for affordably recruiting much-needed talent. There are a number of ways for an employer to start a registered apprenticeship program, and many public resources are available to help. To get started with building or scaling a registered apprenticeship program for youth in cybersecurity, contact the Cybersecurity Youth Apprenticeship Initiative (CYAI) at CYAI2024@icf.com.

Cybersecurity Youth Apprenticeship Initiative (CYAI) is funded by the U.S. Department of Labor's (DOL) Employment and Training Administration (ETA) Office of Apprenticeship (OA). CYAI promotes sustainable development of cybersecurity apprenticeship programs for youth aged 16-21 and is administered by ICF. The goal of the initiative is to create at least 900 new cybersecurity apprenticeships for youth by 2024.