The Need for Cybersecurity in Today's Economy

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 201S: Cybersecurity & Social Science, Professor Trinity Woodbury

March 26, 2025

Assignment:

What does **economics** have to do with **cybersecurity**?

The Need for Cybersecurity in Today's Economy

The readiness economy focuses on providing goods and services that enable organizations to prepare for disruptions, like power outages, cyberattacks, and global pandemics (Redins, 2024). For example, during the COVID-19 pandemic, the Gross Domestic Product (GDP) fell significantly for most countries because many traditional ways of working, producing, transporting, and selling disrupted economies, and no clear indication suggested the world would return to 'normal' (Davis, 2020). Cybersecurity is a critical component of the readiness economy because cybersecurity threats can directly and negatively impact economies and their supply chains. One example is data breaches, which are becoming increasingly common. Organizations can help defend, mitigate, reduce, and hopefully prevent or fully recover from cybersecurity disruption using education and assimilating effective products and services into their current security ecosystems.

Cyber-ready organizations can anticipate, respond, and prevent cybersecurity attacks. Organizations can implement a vast number of tasks to help with that goal. For example, training employees in the best business cybersecurity practices while investing in the latest software and hardware technologies. Other cybersecurity readiness tasks can also include (Redins, 2024):

1. Conducting risk assessments
2. Developing current industry security policies and procedures
3. Ensuring compliance with security regulations
4. Implementing security controls
5. Monitoring and auditing security
6. Conducting mock cyber attacks
7. Keeping cybersecurity insurance up to date
8. Only allowing secure remote access to data for users
9. Implementing multi-factor authentication
10. Running vulnerability assessments regularly

To recession-proof an IT professional's career, exploring and applying for jobs in the readiness economy sector is wise. Over the past eighteen months, many laid-off IT professionals

like software developers and engineers may want to adjust their career path by moving away from their current expertise roles and focusing on an area within cybersecurity. Growing cybersecurity roles and opportunities include security analysts, engineers, and incident response specialists. For example, AI's recent advent and significant growth will require seasoned professionals to monitor the powerful AI technology closely. In contrast, AI monitors and automates many organizations' security and network systems.

Lastly, electric grid security and resilience are another opportunity for IT professionals. Trends for cyber threats are increasing in sophistication, and the threat of a malicious actor attacking our current Supervisory Control and Data Acquisition (SCADA) / Industrial Control Systems (ICFs) is not inconceivable (ICF, 2016). Many SCADAs and ICFs and their protocols are outdated, lacking basic security measures like authentication and encryption, making them "insecure by design." For example, in December 2015, Ukraine suffered a massive remote access attack on its SCADA systems, causing unscheduled power outages and impacting many customers in Ukraine (CISA, 2021). The U.S. attributes the attack to Russian nation-state cyber actors and cyber campaigns from Russia against Ukrainian critical infrastructure. The direct costs for the damage and money lost were never precisely quantified in public records, but the public can estimate and infer the costs in the range of hundreds of thousands to millions of USD. Thus, the role of cybersecurity in an economy is critical and a huge opportunity for IT professionals to make a difference and live in it.

References

CISA. (2021, July 20). *Cyber-Attack Against Ukrainian Critical Infrastructure*. Retrieved from America's Cyber Defense Agency (CISA): https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

Davis, N. (2020, June 1). *What the COVID-19 pandemic teaches us about cybersecurity – and how to prepare for the inevitable global cyberattack*. Retrieved from World Economic Forum: https://www.weforum.org/stories/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/

ICF. (2016). Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats. *U.S. Department of Energy*, 145.

Redins, L. (2024, June 06). *How cybersecurity readiness is good for the economy?* Retrieved from Cybersecurity Guide: https://cybersecurityguide.org/resources/readiness-economy/