CYBERSECURITY THREATS IN THE PHARMACY SECTOR

A Guide Based on the Health Care and Public Health Sector Cybersecurity Framework

Abstract

"Cybersecurity in Pharmacy: A Guide" explores the importance of cybersecurity in the pharmacy sector, detailing the Health Care and Public Health Sector Cybersecurity Framework, recent cyber threats, and best practices for secure operations.

Dr. Gilberto Crespo Pérez

gcrespo@bligconsulting.com

Cybersecurity Threats in the Pharmacy Sector (CTPS)

Executive Summary

The upcoming presentation, titled "Implementing Cybersecurity in the Pharmacy Sector: A Guide Based on the Health Care and Public Health Sector Cybersecurity Framework," aims to provide an in-depth understanding of the importance of cybersecurity in the pharmacy sector. It will highlight the potential risks and impacts of cyber threats, emphasizing the need for robust cybersecurity measures to protect sensitive health data and ensure the smooth operation of healthcare services.

The presentation will offer a comprehensive overview of the Health Care and Public Health Sector Cybersecurity Framework, developed by the U.S. Department of Health & Human Services. This framework serves as a critical tool for healthcare organizations, including pharmacies, to enhance their cybersecurity and cyber risk management programs.

Attendees will gain insights into the detailed components of the framework, including the Framework Core, Implementation Tiers, and the Framework Profile. The presentation will also guide attendees through the recommended seven-step process for implementing the framework, providing practical examples of how each step can be applied in the pharmacy sector.

The presentation will also discuss recent cybersecurity incidents in Puerto Rico and USA, demonstrating the real-world impacts of cyber threats on the healthcare sector. This discussion will further underline the importance of implementing the cybersecurity framework to prevent such incidents.

Finally, the presentation will offer specific recommendations and best practices for maintaining cybersecurity in the pharmacy industry. These recommendations are based on the guidelines provided in the framework and other resources from the National Institute of Standards and Technology (NIST).

The presentation aims to equip attendees with the knowledge and tools necessary to enhance cybersecurity in their respective pharmacy settings. It will conclude with a post-test to gauge the attendees' understanding of the key points discussed during the presentation, followed by a Q&A session for further discussion and clarification.

High Level Outline

1. **Introduction**
    - Welcome and introduction
    - Brief overview of the presentation
    - Introduction to the pre-test questions
2. **Pre-Test**
    - Administer the pre-test questions to gauge the audience's initial understanding of cybersecurity
3. **The Importance of Cybersecurity in the Pharmacy Sector**
    - Explanation of why cybersecurity is crucial in the pharmacy industry (relates to question 1)
    - Recent examples of cybersecurity threats in the healthcare sector (relates to question 2)
    - Reference: National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
4. **Overview of the Health Care and Public Health Sector Cybersecurity Framework**
    - Brief explanation of the framework (relates to question 3)
    - Importance of the framework for the pharmacy sector
    - Reference: U.S. Department of Health & Human Services. (n.d.). Health Care and Public Health Sector Cybersecurity Framework Implementation Guide. https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Documents/HPH-Sector-CSF-Implementation-Guide-508.pdf
5. **Deep Dive into the Cybersecurity Framework**
    - Detailed walkthrough of the framework
    - Explanation of how each part of the framework applies to the pharmacy sector
    - Reference: National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
6. **Cybersecurity Best Practices**
    - Explanation of strong password and multi-factor authentication strategies (relates to question 4)
    - Discussion on controlling access to sensitive data and monitoring the activity of privileged and third party users (relates to question 5)
    - Reference: National Institute of Standards and Technology. (2017). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
7. **Recent Cybersecurity Incidents in Puerto Rico & USA**
    - Overview of recent cybersecurity incidents in Puerto Rico & USA
    - Discussion of the impact of these incidents on the healthcare and pharmacy sectors

8. **Applying the Cybersecurity Framework to Prevent Incidents**
    - Detailed discussion on how the framework could have prevented recent incidents
    - Case studies or hypothetical scenarios demonstrating the application of the framework
    - Reference: U.S. Department of Health & Human Services. (n.d.). Health Care and Public Health Sector Cybersecurity Framework Implementation Guide. https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Documents/HPH-Sector-CSF-Implementation-Guide-508.pdf
9. **Recommendations and Best Practices**
    - Specific recommendations for implementing the cybersecurity framework in the pharmacy sector
    - Best practices for maintaining cybersecurity in the pharmacy industry
    - Reference: National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
10. **Conclusion**
    - Recap of the key points from the presentation
    - Final thoughts and next steps for implementing the cybersecurity framework
11. **Post-Test**
    - Administer the same set of questions to measure the audience's understanding after the presentation
12. **Q&A**
    - Time for questions and answers

References

- National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- U.S. Department of Health & Human Services. (n.d.). Health Care and Public Health Sector Cybersecurity Framework Implementation Guide. https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Documents/HPH-Sector-CSF-Implementation-Guide-508.pdf
- National Institute of Standards and Technology. (2017). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Resource contact information:

Dr. Gilberto Crespo Pérez, DBA, MSCE, CCSA, CIP, CDIA+, ITIL, ECMs, SMGp, SCJP
IT/IS Consulting Services at BLiG Consulting - "Turning Bits Into Meanings"
e-mail: gcrespo@bligconsulting.com
mobile: 787-210-9804
www.bligconsulting.com
www.sapientcoach.com