



## Chapter 19

# Women in Information Technology and Cybersecurity in Healthcare


**Kevin Richardson**

 <https://orcid.org/0009-0002-3212-8669>  
*Capitol Technology University, USA*


**Darrell Norman Burrell**

 <https://orcid.org/0000-0002-4675-9544>  
*Marymount University, USA*

**Calvin Nobles**

 <https://orcid.org/0000-0003-4002-1108>  
*Illinois Institute of Technology, USA*


**Jorja Brittany Wright**

 <https://orcid.org/0000-0002-7028-995X>  
*Capitol Technology University, USA*

**Jennifer Ferreras-Perez**

*Marymount University, USA*

**Amalisha Sabie Aridi**

 <https://orcid.org/0000-0002-7869-5530>  
*Capitol Technology University, USA*

### ABSTRACT

*For a variety of reasons, cybercriminals view healthcare organizations as desirable targets to attack. With significant shortages of employees and managers in cybersecurity and technology management, the need for more professionals in the field have never been more important and necessary. Meeting these workforce development shortfalls and developing innovative business strategies requires leaders from all genders and backgrounds. To effectively meet the most challenging concerns related to organizational technology management strategy will require the contributions of women. This chapter explores the barriers, complexities, and innovative approaches related to developing more women in leadership roles in information technology and cybersecurity in healthcare organizations.*

## INTRODUCTION

Every day, more connected medical devices are being deployed in hospitals by healthcare providers; these medical devices can account for as much as 74% of all the devices that are connected to a hospital's network (Pottinger, 2022). Medjacking is a term that was coined to describe attacks that are specifically aimed at connected medical devices as a result of the prevalence of attacks on medical devices that are hijacked (Pottinger, 2022; Jones, 2022; Peoples, 2022).

These connected devices are frequently required to maintain the patient's life and keep them alive. It is possible that removing their functionality or modifying it in some way could mean the difference between life and death. Like any other digital device, they require regular updates to ensure that they continue to function properly and remain secure (Elam, 2020; Jones, 2022; Peoples, 2022).

Devices such as patient-tracking wristbands, equipment tracking for crash carts, ventilators, portable X-ray machines, and vital-sign monitors are all examples of connected devices (Elam, 2020; Jones, 2022; Peoples, 2022). These devices communicate with one another across the hospital network, supplying medical professionals with important patient information that is entered into electronic health records. The transmitted data enables medical professionals to provide care at lower cost to patients (Elam, 2020; Jones, 2022; Peoples, 2022).

Clinicians can complete their work more quickly and in more secure environments. In addition, each and every device is a potential access point for cybercriminals to take advantage of (Elam, 2020; Jones, 2022; Peoples, 2022). The level of sophistication of cyberattacks, in addition to the severity of the cyberthreat posed to the healthcare industry over the past decade, has significantly increased (Elam, 2020; Jones, 2022; Peoples, 2022). Both business and government have acknowledged the arrival of this new era (Elam, 2020; Jones, 2022; Peoples, 2022). Every improvement brought about by automation, interoperability, and data analytics results in an increase in the vulnerability of the system to malicious cyberattacks (Elam, 2020; Jones, 2022; Peoples, 2022). Cyberattacks are of particular concern for the health sector because they can directly threaten not only the security of systems and information but also the health and safety of patients. This makes cyberattacks a particularly concerning issue for the health sector (Elam, 2020; Jones, 2022; Peoples, 2022).

For a variety of reasons (Elam, 2020; Jones, 2022; Peoples, 2022), cybercriminals view healthcare organizations as desirable targets to attack (Elam, 2020; Jones, 2022):

- The medical and billing information of patients can be quickly sold on the dark web by criminals for the purpose of committing insurance fraud.
- The ability of ransomware to lock down patient care and back-office systems increases the likelihood of receiving lucrative ransom payments.
- Medical equipment that is connected to the internet is susceptible to being tampered with.

According to Elam 2020, Jones 2022, and Peoples 2022, the following are the primary concerns regarding cybersecurity in the healthcare industry:

- Patient information is valuable on the dark web.
- Adequate security controls are frequently lacking in medical devices.
- A lack of adequate training on cyber risks for those working in the healthcare industry
- The use of antiquated technology in many healthcare facilities.

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/women-in-information-technology-and-cybersecurity-in-healthcare/321028](http://www.igi-global.com/chapter/women-in-information-technology-and-cybersecurity-in-healthcare/321028)

## Related Content

---

### A Twofold Approach for Evaluating Inter-Organizational Workflow Modeling Formalisms

Benoit A. Aubert, Aymeric Dussartand Michel Patry (2005). *Business Systems Analysis with Ontologies* (pp. 270-304).

[www.irma-international.org/chapter/twofold-approach-evaluating-inter-organizational/6126](http://www.irma-international.org/chapter/twofold-approach-evaluating-inter-organizational/6126)

### Aggregating and Ranking Method for the Evaluation of Product Design Materials

Daniel Osezua Aikhuele (2019). *International Journal of Operations Research and Information Systems* (pp. 39-52).

[www.irma-international.org/article/aggregating-and-ranking-method-for-the-evaluation-of-product-design-materials/236645](http://www.irma-international.org/article/aggregating-and-ranking-method-for-the-evaluation-of-product-design-materials/236645)

### Business Process Reuse and Standardization with P2P Technologies

José A. Rodrigues Nt, Jano Moreira de Souza, Geraldo Zimbrão, Geraldo Xexéoand Mutaleci Miranda (2010). *Business Information Systems: Concepts, Methodologies, Tools and Applications* (pp. 518-531).

[www.irma-international.org/chapter/business-process-reuse-standardization-p2p/44092](http://www.irma-international.org/chapter/business-process-reuse-standardization-p2p/44092)

### An Extrinsic and Intrinsic Motivation-Based Model for Measuring Consumer Shopping Oriented Web Site Success

Edward J. Garrity (2010). *Business Information Systems: Concepts, Methodologies, Tools and Applications* (pp. 232-251).

[www.irma-international.org/chapter/extrinsic-intrinsic-motivation-based-model/44075](http://www.irma-international.org/chapter/extrinsic-intrinsic-motivation-based-model/44075)

### Optimizing Bundling Policy of Single-Period Products: Perspectives of Producers and Retailers

Gregory Gurevich, Yuval Cohenand Baruch Keren (2014). *International Journal of Operations Research and Information Systems* (pp. 1-25).

[www.irma-international.org/article/optimizing-bundling-policy-of-single-period-products/120445](http://www.irma-international.org/article/optimizing-bundling-policy-of-single-period-products/120445)