Health IT Security Journal

Volume 4, No. 1

A publication of the HITSF

How to Build an Effective Security Team

Health IT Security Journal

Volume 4, No. 1

HITSF

This journal is a publication of the Health Information Technology Security Forum.

The Health IT Security Forum is an International Security Organization that dedicated to help healthcare organization in securing their privacy data, confidential information, medical devices and will be recognized for the passion of its members in conducting multidisciplinary research and development in the area of Healthcare IT Security and e-Health.

Editor in chief: Hadi Syahrial

Review Board

- Eric Vanderburg
- Dr. Nurhizam Safie
- Dr. Moedjiono
- Dr. Lukas

Editorial Board

- Bambang Suhartono
- Gregorius Bimantoro
- Seyed Mohammad Motahar

Letter from the editor

Dear readers,

This is the second year of the Journal and we are proud to present another issue. This issue of the HITSF journal offers insight into information security for healthcare practitioners. We hope you will enjoy it and we welcome your feedback. Please send questions and feedback to editor@healthitsecurity.org

- Hadi Syahrial

Disclaimer

The author(s) of each article appearing in this Journal is/are solely responsible for the content thereof; the publication of an article shall not constitute or be deemed to constitute any representation by the Editors that the data presented therein are correct or sufficient to support the conclusions reached or that the experiment design or methodology is adequate.

IN THIS ISSUE

www.healthitsecurity.org

How to Build an Effective Security Team

by Eric Vanderburg

Security is not an IT function. It is a business area and required a balanced team of professionals from a variety of disciplines. Indeed technical knowledge is needed, but you also need leaders and those with specific knowledge of core business functions in order to have an effective security team. Let's look at them here:

Executive leadership

Effective security teams have top-level support through a member of the C-suite. Their leadership role will prove beneficial to the group, not to mention their thoughts on the security system developed and installed. It is vital that they believe that the system is cost-effective and will not disappoint.

IT staff

These days, an office's security system is linked with the information systems' infrastructure of a company, which means they go hand in hand. The security breach, after all, happens not only offline, but also online. Nowadays, you not only need to keep an eye on who walks through the door, but also on who has access to your network. This only shows that a member of the IT department must be included in a security team, whether security system is managed in-house or outsourced.

It is important to note, however, that the IT department should not dictate which security system should be used company-wide. They should take care of the virtual security and leave the physical security to the security department.

Human Resources

Who better knows employment laws, company policies and other labor rules than human resources (HR)? They can help ensure that the security team was not violating any laws when they developed or implemented a system. Moreover, there is an important link between security and HR where employees are concerned. The moment a new hire is on board, he will be added to the security system right away. If anyone gets fired, he will be removed from the system just as quickly. HR is also responsible for creating security measures, such as questioning anyone without a name badge or prohibiting them from accessing certain areas of a storage network.

Finance

Apart from the fact that money is needed to implement a security system, a representative of the finance department can also ensure that a plan is made and the steps taken will have a positive impact on a company's bottom line. Security, after all, is not the only thing that a business has to spend on. It is vital that the security system implemented proves to be a lucrative investment, rather than a money pit.

Now that the team members have been selected, it is time to take steps to ensure a security team functions as intended.

- Security challenges must be identified, so solutions to address them will be formulated
- Reduce security risks, such as online and offline breach
- Perform ongoing and regular maintenance
- Choose a system that provides most value, and can be leveraged across multiple departments

About the Author:
Eric Vanderburg

Director, Information Systems and Security,
JurInnov Ltd.

Eric Vanderburg understands the intricacies inherent in today's technology and specializes in harnessing its potential and securing its weaknesses. He directs the efforts of multiple business units including Cyber Security, eDiscovery, Computer Forensics, Software Development, IT and Litigation Support at JurInnov, an eDiscovery and eSecurity consulting firm. Vanderburg holds over thirty vendor certifications and is completing a doctorate in information assurance. He has dedicated much of his career to designing and implementing systems, policies and procedures to enhance security, increase productivity, improve communications and provide information assurance. He has been invited to speak at conferences and events on technology and information security and he is active in promoting security and technology awareness through various publications.