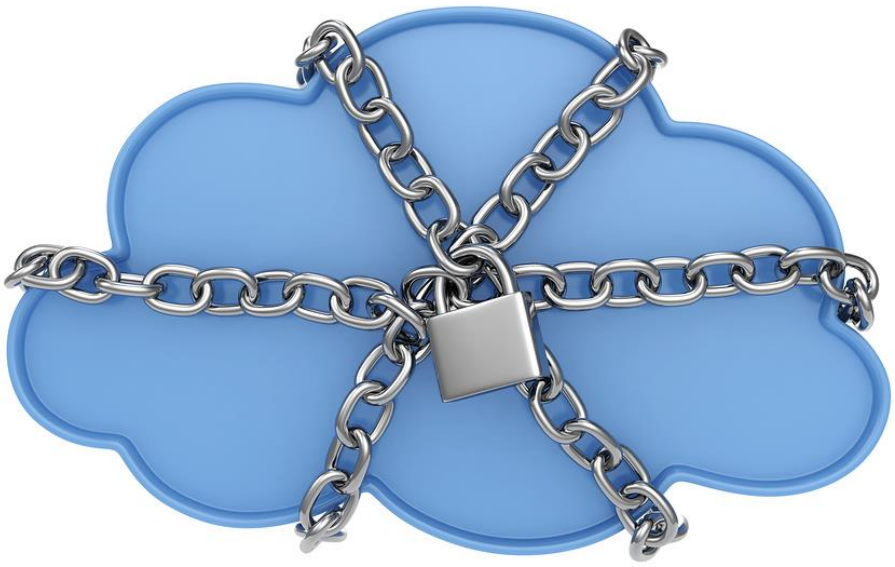
Health IT Security Journal

Volume 2, No. 4

A publication of the HITSF

Effective storage security strategies for enterprise data

BYOD policy elements



Health IT Security Journal

Volume 2, No. 4

HITSF

IN THIS ISSUE

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.

www.healthitsecurity.org

Effective storage security strategies for enterprise data

by Eric Vanderburg

Data breaches are one of the biggest problems that companies face. According to the 2014 Data Breach Investigations Report by Verizon, there are 92% confirmed data breaches in 2013. In the case of Sony being hacked, there are more than 101 million records that were breached, but mostly email addresses. But a really worrying fact is the 273 breaches that involved over 20 million sensitive personal records. Whether directly affected or not, businesses and individuals have something to worry about.

But a breach can be prevented, and companies can certainly do something to protect their own data and those of their customers. What storage security strategies can enterprises implement?

Classify data accordingly

Some details can be shared, while others are classified as confidential. It is vital that there is a consistent and effective process of identifying and classifying data, so that data privacy is achieved. This should include determining different confidentiality levels of data and different data access models, identifying and categorizing sensitive data, and figuring out where sensitive information must be stored.

Develop a security policy

The best security policy is one that defines how an organization must address constraints in data storage, and outlines how to protect its physical and information technology assets. There are several essential points that must be considered, such as acceptable threat level, authentication and authorization policies, and compliance measures. It is vital that a data is encrypted early on in its life cycle, and whatever policies implemented in terms of security, must follow best practices and comply with legislative measures that best suit your company.

Implement data privacy

Solutions to protect data from breach can be done at multiple points. Identifying these points will influence the overall storage security model of your enterprise, which is why different implementation modes must be identified.

- Encryption at storage level

This refers to security measures where data is encrypted at the file level. Encryption is done on tape media, storage blocks, and directories. But because such media are still vulnerable to theft, storage-level encryption must ensure that when tape media or storage blocks are stolen, for instance, the content would be useless to thieves.

- Encryption at network level

Considering that data is passed over the internet to customers, partners and other entities, the network-level encryption is the highest and most secure of data privacy solution. Aside from using technologies, such as SSL and IPsec, data are also parsed and sensitive elements are encrypted to ensure that even if transmission is compromised, privacy is still maintained.

- Encryption at application level

This is essential for keeping credit cards, health records, or e-mail addresses secure at the application tier. With an application-level encryption, data is protected against database and storage attacks, including storage media theft, so there will be no worries when such data are processed, authorized or manipulated.

There are many other storage security strategies that a company can use, but building blocks of data privacy solution must be prioritized, such as backup and recovery, hardware protection, authentication and authorization, and logging, auditing and management of encrypted data.

About the Author:
Dr. 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. Look for his latest book, "Storage+ Quick Review Guide", due for publication with McGraw Hill in December of 2013.

BYOD Policy Elements

by Ramana Gaddamanugu

It is not unusual for companies these days to give a stipend for employees to purchase technology or bring their own devices to work. After all, the work environment has changed so much that most employees tend to bring their work at home with them. This means that they have to sync office information with their own devices in order to continue working outside of the office.

While it has its own conveniences, there are also many security implications. The most glaring of which is that company information is being taken out of the office premises and being brought to an area where it becomes much more vulnerable.

In order to minimize or avoid trouble altogether, a BYOD policy needs to be put in place. This is so that usage of such devices can be controlled and security risks are easily mitigated. Certain elements should be in your BYOD policy and these include:

Establish which devices can be brought in

While it's pretty easy to say that you can bring in "your personal device," you have to be much more clearer than that. Specify exactly what devices are allowed. For example, are you going to support iOS devices only? How about Android devices? Is the iPhone acceptable? How about tablets?

Being clear on what can and can't be used so that there wouldn't be any arguments when it comes to devices.

Do not allow jailbroken and rooted devices

These devices are already compromised and it's just risky to have them connected to your computers and networks. So, it's best to not allow these kinds of devices to be attached to your systems.

Require the use of screen lock passwords

While some consider the addition of passwords to be a hassle, it's one of the best ways to prevent unauthorized access of data. Your policy should feature this and it should be strictly implemented.

You can also be extra strict when it comes to the type of password that should be used. We've been told time and again that a good password is always a lengthy one comprised of characters, letters and numbers.

Be clear on the service policy for personal devices

It's natural for devices to falter once in a while. When it happens, do you provide service to fix it? Will you provide devices on loan so users can continue working while you repair their personal one?

Outlining what can and can't be done sets boundaries and helps avoid unnecessary arguments later on.

Make sure about who owns what data

Personal phones contain photos, videos, notes and other items of a personal nature, as well as items that a user has personally paid for. What happens when that device is lost or stolen? For example, iOS devices can be wiped clean in the event of theft or loss. Wiping the device means erasing EVERYTHING and some of those are really hard to replace like photos.

On your part, you can clearly state that data in the devices brought to your premises are yours. Meaning, you can wipe it off when there is a need for it. But since this is the case, you also have to provide a backup procedure for users so they can restore their phone once they find a replacement.

Have an exit strategy in place

It's common for employees to leave and you have to ensure that the information and other access they have are completely removed from their personal devices. Whether you choose to completely wipe the personal device or disable access, be clear on what will be asked of them when they leave. This way, you avoid potential problems when exit time comes.

The workplace has changed, that much is true. But this doesn't

mean that security needs to be lax. This is why if you're a company that will allow the bringing in of personal devices, then you must enforce guidelines to ensure the safety of your data. After all, it is

About the Author:

Ramana Gaddamanugu

Ramana Gaddamanugu is a privacy and fraud expert. He is a certified fraud examiner and a chartered accountant.