Health IT Security Journal

Volume 3, No. 4

A publication of the HITSF

Health IT Security Journal

Volume 3, No. 4

HITSF

www.healthitsecurity.org

IN THIS ISSUE

Physical Security for Data in Transit

by Eric Vanderburg

Technology does not provide answers to cybersecurity problems

by Ramana Gaddamanugu

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

Physical Security for Data in Transit

by Eric Vanderburg

Briefcase chained to his wrist, the officer cautiously looks for anything out of the ordinary as he makes his way purposefully to a black vehicle with government plates. You would think he might relax with two armed men flanking him and another waiting at the car but his rigorous training keeps him focused. The thought of the coded orders he protects falling into another's hands reminds him of the need to stay alert.

The scene depicted here highlights the importance the government places on data being transported. Organizations also transport valuable data but too often little is done to protect it. The scene above is an extreme case. Shareholders do not expect companies to go to that same length to protect each hard drive or backup tape but they do expect reasonable physical security measures to be taken to protect data in transit.

Physical security is a major component of information security. Physical security encompasses the actions taken to prevent attackers from accessing equipment, facilities, and other resources where data is stored, shared, or worked with. Physical security is often likened to a castle. Whereas a castle has tall walls, a moat, drawbridge, gate, guards, and lookouts, physical security systems likewise have cameras, sensors, guards, walls, authentication devices, GPS, and many other technologies.

Physical security needs to be in place for assets in transit. For example, a store manager wouldn't toss bundles of cash into his trunk to transport to the bank. This would be much too risky. Rather, the money is picked up by armored car. Why then is valuable data often transported with little or no thought to security? The evidence of such activity is profuse…stolen tapes, lost hard drives, and flash drives containing valuable company information or private customer data fall into the wrong hands, making headlines in the process.

This is why organizations need to recognize the importance of physical security, not only for data in facilities, datacenters, offices, or storehouses, but in situations where devices containing data are being transported. Such situations might include transporting backup tapes off-site or distributing data on optical storage or flash media.

This article looks at ways to provide physical security for data in transit. Physical security protects against incidents such as:

- Backup tape damage
- Hard drive damage
- Media theft
- Media interception
- Media duplication

Backup tape damage

Backup tapes are a form of magnetic media and they can be easily damaged. Electromagnetic waves can scramble the data on a tape or physical impact, such as dropping a tape, can damage the media or mechanisms inside the tape housing. Organizations should protect against backup tape damage by requiring tapes to be stored in their plastic clamshells and to be transported in a padded case.

Those transporting tapes need to be careful not to expose the tapes to magnetic fields or devices that generate large amounts of electromagnetic waves such as speakers or subwoofers. Those handling tapes should be trained not to touch the magnetic media inside the tape as oils from a person's skin will interfere with the ability of backup devices to read and write to the tape.

Lastly, tapes should be protected against the elements. The transport case should be water resistant in case tapes are transported in the rain.

Hard drive damage

Similarly, hard drives need to be protected in transit. A hard drive is made up of round platters that store data on both sides. Small devices called heads glide very close to the surface of these platters to read the information stored on the magnetic platter. If a hard drive is impacted or jolted back and forth these heads may scrape against the platter damaging the data stored in those locations and possibly the head as well. Care should be taken when transporting hard drives. Drives should be transported in protective cases to

protect the drive to some degree from shock if the drive is dropped.

Drives can also be damaged by static electricity. People absorb and discharge electrons as they come into contact with other objects. Normally the absorption or discharge is too small for a person to take note of but occasionally a person might feel a static shock. Computer equipment can be damaged by a much smaller amount of static electricity so a person could damage the electronics in a hard drive without even knowing it. Antistatic bags decrease the chance of static electricity being discharged into the drive electronics and they should be used whenever a drive is transported.

Media Theft

Theft is a concern for media being transported, be it tape, hard drive, flash drive, or some other storage device. Controls in this area could be as simple as locks on tape or drive transport units or something more complex like GPS tracking devices or switches that demagnetize media if stolen. Additionally, the transport method could be obscured to make thieves unaware that data is being transported. Transport devices could be made to look like a standard briefcase or, if small enough, could be slipped inside a backpack.

Pictures and names of employees authorized to transport media should be provided to locations that have guards on duty and those guards should check identification before allowing personnel to leave carrying media.

Media interception

Media interception is another area where physical controls are needed. If data is sent via postal mail, ensure that mailboxes can be opened only by postal service workers. Media packaging should be tamper resistant. Such packaging can only be opened once because the process of opening the package renders it useless. After that the package cannot be reassembled without providing clear evidence of the tampering. Tracking should be used on packages and a signature required upon receipt.

Media duplication

Thieves want to obtain the data on such media and access to the media for a sufficient amount of time could provide an opportunity for a copy to be made. For this reason, those transporting media should not make unrelated stops along the way to their destination. This means no coffee breaks, window shopping, or picking up groceries along the way. Needless to say, media should not reside in an insecure location on its way to the destination such as storing tapes in the trunk of a car while picking up kids from school or leaving a hard drive in a briefcase overnight to avoid an extra trip to the office. These situations create opportunities for theft. Controls in this area can take the form of transport procedures, sign in and sign out procedures and audits to ensure that media leaves and arrives in the appropriate amount of time. Transports that take too long could be cause for concern.

Summary

This article introduced physical controls for protecting data in transit from damage, theft, interception, or duplication. Most of the controls mentioned here can be implemented at nominal cost and they will provide much greater security for data in transit. Along with these physical controls, operational controls should be implemented to enforce usage of the physical controls and those transporting data should be trained on the use of physical controls.

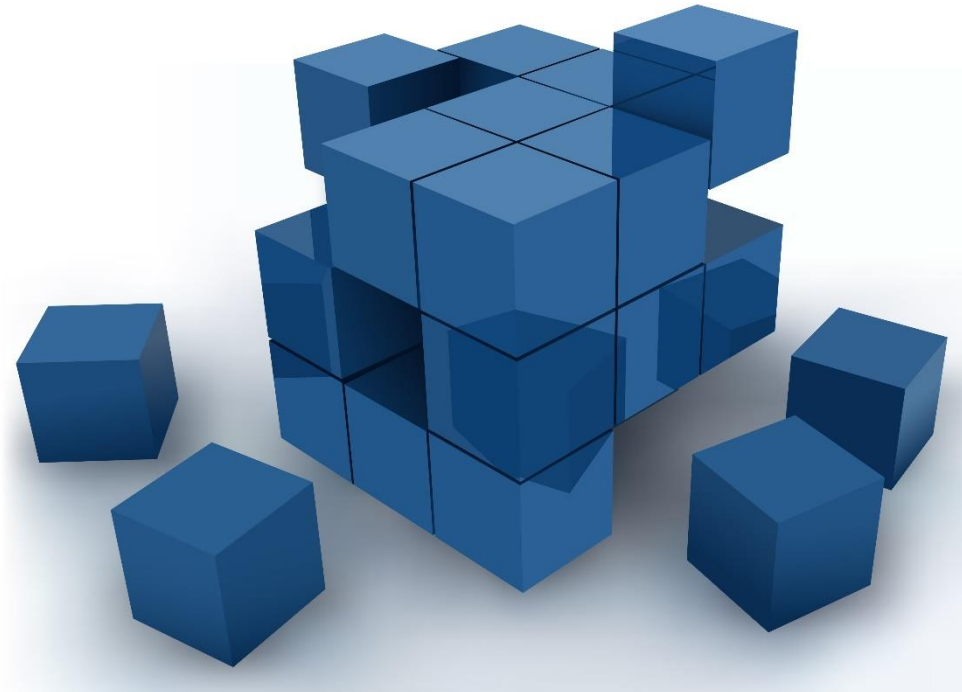
About the Author:
Eric Vanderburg

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.

Technology does not provide answers to cybersecurity problems

by Ramana Gaddamanugu



As more of the tasks and actions that make up our everyday lives move into the digital space, sophisticated computer networks and information systems drive our world, enabling better and simpler access to everything from critical infrastructure and national security to online shopping and education.

The free and open internet has supported immense growth in economies worldwide and facilitated unprecedented information flow from the largest cities to the most remote (and previously unreachable) places on Earth. But as they become increasingly indispensable, the digital systems powering our world also become prime targets for attack from groups and individuals spanning from well-organized cyber-crime gangs to state-supported hackers.

With internet access rapidly expanding across the globe, and the proliferation of greater connectedness across business, finance, and individuals, ensuring privacy and security of this activity will only become more paramount.

This reality makes cybersecurity – the technologies, processes and best practices that protect networks, individual computers, programs and all digital data from attack — one of the critical problems of our time.

Despite public and private sector investments in sophisticated security systems, the level of risk continues to rise on par with innovations. Developing impenetrable security forces online in the face of ever-advancing modes of attack, exemplified by the myriad of well-publicized, increasingly sophisticated data breaches affecting multinational corporations, organizations and governments, is the great arms race of the 21st century.

As security professionals, companies and academics look for answers, efforts have been heavily skewed toward finding technological solutions. Yet, experts estimate that between 70-80% of the cost attributed to cyber-attacks is actually a result of human error. Things as simple as clicking on a bad link, opening the wrong email attachment, or using an insecure USB drive can be devastating to network security. The strongest security network in the world is only as good as the human with the password.

Human error is not limited to end users. Computer engineers may develop code in ways that compromise the security of their software, IT administrators may not set up security systems properly, and CEOs may make the wrong investment decisions when it comes to security infrastructure. The challenges around understanding and addressing human behavioral factors in cybersecurity present a rich vein of opportunity for making the system as a whole more robust.

About the Author:

Ramana Gaddamanugu

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