Health IT Security Journal

Volume 3, No. 3

Essential elements of an incident response plan

How trust can influence business productivity and security

A publication of the HITSF

Health IT Security Journal

Volume 3, No. 3

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 can be recognized for the passion of its members in conducting multidisciplinary research and development in the area of Healthcare IT Security and e-Health.

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 can 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

Essential elements of an incident response plan

by Eric Vanderburg

After a hack or security breach (called an incident), appropriate actions need to be made to limit the damages and reduce recovery time and costs. The steps to take after such an incident is laid out in an incident response plan. In that document, detailed steps on the process to follow after an incident should be outlined.

Your organization's computer incident response team is tasked with coming up with an incident response plan. Members of that team can include security and general IT staff, as well as representatives from legal, human resources and public relations departments.

After the development of the incident response plan, this should be reviewed annually to reflect changes to certain policies, processes and technologies used within the organization.

User and system administrators need to be aware of incident response procedures so that prompt actions can be taken to prevent further damage or at least reduce it.

Different Types of Security Incidents

Security incidents can involve the following:

- Violation of computer security policies and standards
- Unauthorized computer or data access
- Presence of viruses and other malicious applications
- Presence of unusual programs
- Misuse of service, systems and information
- Physical or logical damage to systems
- Computer theft

Details on local incident response team and their responsibilities

You should have the names and contact details of the incident handler and the resource manager, as well as their responsibilities on file. The former is the security contact who has system administrator credentials, technical knowledge of the system, as well as knowledge of the location of the incident response plan. If an alternate contact is available, their details need to be on record as well.

The latter refers to a decision maker for the system. They understand the impact of the system on the business and its unavailability.

Details on the system

This portion should include reference to the location of system details. They can be in the form of:

- data flow diagrams
- network diagrams
- system hardware inventory
- logging information

Process to follow when reporting and handling an incident

This is where you outline your response plan from start to finish. It's important that everything listed here should be detailed. A sample flow could go:

- File an incident report containing the following information
- name and phone number of person who's system may have been breached
- IP address, hostname and physical location of said system
- impact of incident (what data may be compromised and which other users can be affected)
- description of incident (what activities were done when the incident was noticed or how the incident was detected)
- Report incident to proper authorities
- Take action to solve the incident

There are different levels to certain incidents and its impact needs to be assessed. The following factors can be used as measurement:

- the effect of the incident on functionality if affected system
- does the incident breach confidentiality or integrity of data
- is the entire population affected by the incident
- what is the impact of the incident on the reputation and finances of the organization

Security breaches are no laughing matter for a business. They can compromise valuable information and cause disruption within an organization. But with an incident response plan, damages can be minimized when the right steps are taken to address it.

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

How trust can influence business productivity and security

By Ramana Gaddamanugu

Trust is when you rely on another person's integrity and strength. You trust them to do the right thing under any circumstances. With trust you can put yourself on the line and not be afraid that the other person would sell you out or leave you battered and bruised.

In a corporate setting, trust among members makes for an effective team. The sense of safety that everyone feels makes it easy to open up, expose vulnerabilities and take appropriate risks. So what happens when trust is nonexistent?

Productivity can suffer

Rather than work hard to get the job done, employees would be constantly on their toes and hesitant to do something that would have proven beneficial for everyone and the company. They would spend their time protecting themselves and their interests. This result in deadlines not met and goals not realized.

The lack of trust can also lead to low employee morale that can result in counterproductive behavior, lack of ownership over their work, and high employee turnover. Worse, when employees leave, they take with them the knowledge, skills and abilities that can help another organization improve their goals, profit and performance.

Progress can be stunted

Some of the greatest ideas come from employees who are not part of the executive team or a board member, but if they don't trust their leaders and managers to respect their ideas and receive it with respect, they would rather keep their ideas to themselves than share it. Along with the lack of open communication, a company could be stuck with the same idea. Any opportunity to move forward or to innovate would be hampered with the lack of collaboration and communication.

Security can be questioned

Trust is just as important between the company and its customers. So what happens if they can't trust your business' security, whether online or offline? A recent study showed that shoppers are wary of companies that have experienced security breach. Even if they have improved their security system, client would be hesitant to transact with them again. Sure, trust can be regained, but it would take a long time for customers to gain trust on your security again. Victims, on the other hand, would probably never do business with a breached company again.

Firms that are also vulnerable to cyber-attacks can suffer the same fate. No customer would do business with an entity that would be unable to protect them against identity theft, fraud and virus attacks.

This is why establishing trust on the get-go is vital to any business, whether it is trust among employees, between employer and employee, and between a company and the client. The lack of it is simply not an option. A lot of big corporations, and even empires crumbled due to the lack of trust.

About the Author:

Ramana Gaddamanugu

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