Health IT Security Journal

Volume 1, No. 4

A publication of the HITSF

Avoiding the corporate espionage data breach

Business Continuity Management (BCM)

Health IT Security Journal

Volume 1, 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 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

Avoiding the Corporate Espionage Data Breach

by Eric Vanderburg

The term "corporate espionage" often evokes images of big evil corporations, the latest high tech equipment, and skillfully trained spies. Such images have been reinforced through the narratives of movies like "The Net" and "Disclosure," which were widely popular during the 90's when the advancement of the Internet was underway. Still, as exciting, disturbing, and real as some of these movie scenarios seemed, the Hollywood fare seemed a far cry from the everyday mundane world of work that occupies the reality of most corporations, making the threat of corporate

espionage of little concern for most organizations – and one far more suited to the screenwriters or top-selling authors such as John Grisham. Yet, the truth is that neither view is accurate. While corporate espionage requires none of these ingredients – no menacingly evil corporation, no spy vs. spy theatrics, not even high tech equipment – it is a very real threat in the everyday life of organizations everywhere.

Defining the Threat

Simply put, corporate espionage, also referred to as industrial espionage or economic espionage, is the theft of company information. It is conducted for the purposes of obtaining trade or other sensitive information by usually dishonest means, although not always illegally. Although corporate espionage is sometimes conducted at the request of other corporations, it is more often than not conducted by employees and others within the organization. Successful attacks leave companies unaware that information has been stolen; and the incidents that are discovered are frequently handled quietly in order to avoid negative publicity or future occurrences that could arise when an already-attacked company looks like an easy target.

In other cases, stolen information is sold to the highest bidder or ransomed back to the organization. In a case from June, 2012, a medical practice had one of its servers encrypted, preventing them from accessing over 7,000 patient records, only to later be served with a ransom demand for an undisclosed sum. In a 2007 survey published by the American Society for Industrial Security (ASIS), the financial impact of individual espionage cases ranged from less than $10,000 to over $5 million dollars *per* incident. In one of the worst cases of corporate espionage, Canadian technology giant, Nortel Network, was bankrupted and had its assets sold off.

Unveiling the Face of Corporate Espionage

At the core of all espionage is the human element. Before any technological wizardry, a person gathers information. The espionage itself is focused on people and not necessarily about defeating technology. According to Edward Hurley, Assistant News Editor at Search Security, "Often the weakest link in security is not technology, but the people who use it."[1] Attackers known as social engineers gain the confidence of employees within an organization and then persuade them to obtain information on their behalf. In this way, the technology in place to prevent outsiders from gaining access to confidential information often is circumvented. Social engineering does not attack the technology directly; instead, social engineers have a multitude of resources at their fingertips to manipulate and infiltrate the organization's infrastructure. While certain individuals might be more vulnerable to being used by social engineers, including people with substance or gambling addictions; anyone is susceptible, including individuals with more commonplace problems such as financial or marital troubles. Single or lonely people might be invited into a friendship. Sometimes, it is nothing more than people trying to be helpful. To emphasize the importance of people as opposed to technology, in a recent hacking contest, a WalMart manager was exploited to reveal the details of a Walmart store's operations and layout, all part of a competition where the participants had to obtain a specified number of key elements to win. The only tools used were a telephone and some clever acting ability – no special training or high tech gadgetry and certainly no cloak-and-dagger shenanigans.

The process starts with information gathering. Social engineers utilize Internet searches and social networking sites to learn about company employees. They gain personal information that allows them to gain the trust of an individual. They might pretend to be a person from their past, share a common interest, or just get to know the person, all without revealing their true identity or purpose. Once trust is gained, the social engineer exploits that trust to obtain access to information or other individuals.

Sometimes corporate espionage involves admitting the wrong person into the workplace – hired or otherwise. In large

organizations, a non-employee suddenly occupying a once empty cubicle may go unnoticed, since most employees will not know every other employee, nor is it rare for companies to employ contract or temporary workers. Such scenarios can prove to be dangerous, as the real employees may readily share information with the "mole." When the rogue person has been hired, that proves to be an even more difficult situation. Thus, performing background checks on all prospective employees is an integral component in preventing corporate espionage.

Reducing the Threat of Corporate Espionage

Keeping in mind the definitions of corporate espionage and social engineering as described above, there are some positive steps to take in preventing such threats. First, educating employees is essential in any efforts to obstruct the advancement of corporate spies. Part of this education must include reviewing cases of past espionage experiences that have occurred within the organization, as well as reviewing relevant cases that have occurred in other organizations. Secondly, employees should be instructed in social networking awareness in order to recognize how their personal posts and tweets on social networking sites can adversely impact their organizations. Finally, members of the organization must recognize the role that physical security plays in combating corporate espionage.

One of the first elements in educating employees is for them to recognize the sensitivity of the information they encounter on a daily basis. Employees are not always cognizant of the ways that data can be exploited by corporate spies, even data that seems rather trivial. An emphasis should be made on keeping all company information private and never sharing it, even with individuals who are believed to be trustworthy. It is paramount that employees confirm a person's identity before access is given to usernames, passwords, or other "classified" information. Employees can also be instructed to be on the lookout for behaviors or other signals that mimic past espionage attempts. Besides providing examples of actual cases, creating hypothetical cases is another good way to help employees think outside of the box.

Social networking is ubiquitous and certainly here to stay. With the increase in the number of social networking sites, people have been able to maintain contact with their friends. This contact also indirectly links them up with the friends of their friends as well, further broadening the informational circle. Closer to the world of business, social networking sites allow organizations to advertise their brand as well as their own unique culture. Such sites can have very positive effects, but they also open the door to dangerous risks for organizations and their employees. In order to undermine a company, spies need time for research, but what used to take hours or days now takes minutes for uncovering sensitive information posted on sites such as Facebook or Twitter. Thus, employees need to be educated about the possible pitfalls of social networking sites and be well versed in the difference between positive advertising and negative broadcasting.

Along with the risks that go with such non-physical constructs, it is still essential that attention be paid to risks with physical security. Visitors should always be escorted and kept under close supervision. They should not be able to access computers or work in areas where private information is accessible. Safeguards can be as simple as having employees ensure that information is never left unsecured on untended desks or computers. Not only should access cards be required at all entrances, but employees should be strictly discouraged from sharing access cards with co-workers, other employees, friends, or family members. Seemingly harmless contractors may be interested in far more than helping one's organization. Although simple and easy to adopt, the use of these mitigation techniques can drastically reduce the threat of corporate espionage.

Corporate espionage is a real threat. As indicated, unlike the very common – and wrong – perceptions that it involves elaborately trained spies using high tech skills to gain information, it is far more concerned with people than technology. People are not only the key to obtaining information, they are also the key to protecting information. Consequently, when employees have been armed with these strategies, organizations can better protect themselves against the threat of corporate espionage and the unauthorized disclosure of information.

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.

Business Continuity Management (BCM)

by Hadi Syahrial

Business continuity management is critical for organizations of all sizes and industries. Without business continuity management, an organization will simply not be able to operate effectively, or at all, in the days following a natural or man-made disaster.

This becomes even more important in industries such as healthcare. Healthcare organizations need not only to be able to manage the disruption that such incidents create, but also to have plans to ensure that the service to patients and others continues with the least possible danger, hardship or inconvenience. The loss of a computer system may have serious consequences to out-patient clinics and the loss of a facility because of fire will necessitate other arrangements being in place to ensure business and service continuity.

If a small retailer has to shut down, it may lose profits and customers. If a hospital has to shut down, it may lose lives. That is why it is essential for healthcare providers to develop and implement thorough, effective business continuity management.

Business continuity management is a framework for identifying an organization's risk of exposure to internal and external threats. The goal of BCM is to provide the organization with the ability to effectively respond to threats such as natural disasters or data breaches and protect the business interests of the organization. BCM includes disaster recovery, business recovery, crisis management, incident management, emergency management and contingency planning.

ISO 22301, the world's first international standards for Business Continuity Management (BCM), has been developed to help organizations minimize the risk of such disruptions. ISO has officially launched ISO 22301, "Society security - Business Continuity Management System – Requirements", the new international standard for Business Continuity Management System (BCMS).

According to ISO 22301, a business continuity management system emphasizes the importance of:

- Understanding continuity and preparedness needs, as well as the necessity for establishing business continuity management policy and objectives.
- Implementing and operating controls and measures for managing an organization's overall continuity risks.
- Monitoring and reviewing the performance and effectiveness of the business continuity management system.
- Continual improvement based on objective measurements.

What is Business Continuity Management (BCM)? BCM is a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

A BCMS, like any other management system, has the following key components:

a) a policy;
b) people with defined responsibilities;
c) management processes relating to
    1. policy,
    2. planning,
    3. implementation and operation,
    4. performance assessment,
    5. management review, and
    6. improvement;
d) documentation providing auditable evidence; and
e) any business continuity management processes relevant to the organization.

ISO 22301 is organized into the following main clauses:
Clause 4: Context of the organization
Clause 5: Leadership
Clause 6: Planning
Clause 7: Support
Clause 8: Operation
Clause 9: Performance evaluation
Clause 10: Improvement

Each of these key activities is listed below.

Clause 4: Context of the organization

Determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the expected outcomes of its BCMS such as:

- the organization's activities, functions, services, products, partnerships, supply chains, relationships with interested parties, and the potential impact related to a disruptive incident;
- link between the business continuity policy and the organization's objectives and other policies, including its overall risk management strategy;
- the organization's risk appetite;
- the needs and expectations of relevant interested parties;
- applicable legal, regulatory and other requirements to which the organization subscribes.

Clause 5: Leadership
Top management needs to demonstrate an ongoing commitment to the BCMS. Through its leadership and actions, management can create an environment in which different actors are fully involved and in which the management system can operate effectively in synergy with the objectives of the organization. They are responsible for:

- ensuring the BCMS is compatible with the strategic direction of the organization;
- integrating the BCMS requirements into the organization's business processes;
- providing the necessary resources for the BCMS;
- communicating the importance of effective business continuity management;
- ensuring that the BCMS achieves its expected outcomes;
- directing and supporting continual improvement;
- establish and communicate a business continuity policy;
- ensuring that BCMS objectives and plans are established;
- ensuring that the responsibilities and authorities for relevant roles are assigned.

Clause 6: Planning
This is a critical stage as it relates to establishing strategic objectives and guiding principles for the BCMS as a whole. The objectives of the BCMS are expression of the intent of the organization to treat the risks identified and/or to comply with requirements of organizational needs. The business continuity objectives must:

- be consistent with the business continuity policy;
- take into account the minimum level of products and services that is acceptable to the organization to achieve its objectives;
- be measurable;
- take into account applicable requirements;
- be monitored and updated as appropriate.

Clause 7: Support
The day-to-day management of an effective business continuity management relies on using the appropriate resources for each task. These include competent staff with relevant (and demonstrable) training and supporting services, awareness and communication. This must be supported by properly managed documented information.

Clause 8: Operation
After planning the BCMS, an organization must put it in operation. This clause includes:

- Business Impact Analysis (BIA)
- Risk Assessment
- Business Continuity Strategy
- Business Continuity Procedures
- Exercising and Testing

Exercise type:

- Checklist
- Structured Walkthrough
- Simulation
- Parallel
- Full Interuption

Clause 9: Performance evaluation
Once the BCMS is implemented, ISO 22301 requires permanent monitoring of the system as well as periodic reviews to improve its operation:

- monitoring the extent to which the organization's business continuity policy,

objectives and targets are met;
- measuring the performance of the processes, procedures and functions that protect its prioritized activities;
- monitoring compliance with this standard and the business continuity objectives;
- monitoring historical evidence of deficient BCMS' performance conducting internal audits at planned intervals;
- and evaluating all this in the management review at planned intervals.

Clause 10: Improvement
Continual improvement can be defined as all the actions taken throughout the organization to increase effectiveness and efficiency of security processes and controls to bring increased benefits to the organization and its stakeholders.

About the Author:

Hadi Syahrial

Hadi Syahrial is a Lecturer and Researcher at Budi Luhur University, Jakarta, Indonesia.