Published on *Medical Electronics Design* (http://www.medicalelectronicsdesign.com)

Multilayer Information Protection Methods

Frank Pisciotta
Created *2012-07-11 12:59*
[1]

Multilayer Information Protection Methods [2]

July 11, 2012
By: Frank Pisciotta

Find more content on: Feature [4] Technology [5]

Tips to get started securing your weakest link in information protection, which may not be what you would expect.

Physical security is often overlooked by organizations as they seek to protect their electronic information. There is an old adage that you are only as strong as your weakest link. This applies to the convergence of IT security and physical security. Regardless of how secure your IT data may be to hackers, it is no match for someone who gains access to your servers through a laptop stolen from an employee's car or a table at a coffee shop.

One security integrator tells the story of being on a tour of a large software company. The IT security manager brags throughout the tour about the security of their digital information. As they approach the server room, the guide lifts a piece of paper with a cartoon on it to reveal a hole through which he reaches and opens the door to the server room. Your digital information is only as secure as your weakest link.

Consider if the room is accessible only through key cards, but you lack video cameras recording who enters the room. A stolen access card or well-timed entry behind another employee provides a disgruntled employee unseen access to your data which is exposed to download or corruption. There are countless anecdotes of IT security being compromised through a lack of physical security.

According to the 2011 Ponemon Institute's annual study of data loss, the costs of data breaches dropped in 2011 for the first time in seven years.[1] Francis deSouza of Symantec observes, "This year's report shows that insiders continue to pose a serious threat to the security of their organizations. It is essential for companies to put the proper information protection policies and procedures in place to counterbalance these new realities."

While the average cost per compromised record decreased, internal negligence remains the main cause of data breaches. In 2011, this cost a company $194 per compromised record. Contributing to organizational costs, the company loses business at a rate of 3.7% customer loss to a security breach.[2] Consider how much investment takes place to increase your customer base by 3.7%.

The reports also notes that companies that increase security through external consultants and internal information security officers can see a $41–$80 drop per record in security breaches. To estimate cost of a data breach to your company, there are multiple methods. Two resources calculators available are Symantec and Information Shield.[3,4]

As you consider the importance of IT security and the costs of having it breached, there are two facets to keep in mind to protect information, IT security, and physical security. This article will provide tips to get started securing your weakest link in information protection, which may not be what you would expect.

Information Technology

Information technology controls are clearly necessary to protect sensitive digital information. Ensuring encryption, passwords, and other access barriers to the data will help keep it safe from ill intent. James Kelton, managing principal of Altius IT [6], an IT security audit and security consulting firm, knows well the importance of information technology and what it takes to protect electronic information.

A mid-size medical product manufacturer was concerned about the security of a new device and contacted Jim's organization for assistance. The manufacturer was concerned about patient confidentiality and the integrity of the product. Quite a bit of investment had gone into the development and research to date on the product. Altius IT provided a security risk assessment. The risk assessment inventoried relevant assets and assigned the assets to asset categories. They identified specific threats and threat categories. Then they identified and documented vulnerabilities that existed as a result of the threats. Their risk analysis evaluated risks including the likelihood of various threat exploits. Then they identified security gaps that could be exploited by insider and outsider attacks.

Altius IT's risk treatment plan identified risk reduction and risk treatment safeguards and controls for each vulnerability. Their risk task list identified preventive, detective, and corrective controls that eliminated or reduced risks to acceptable levels. Residual risks,

risks that existed after controls were implemented, were identified and prioritized so that they could be monitored. Altius IT performed various testing scenarios to ensure the products had been appropriately hardened.

Now consider the risk assessment process from a physical security perspective. First the physical security consultant would work with the client to identify and classify critical assets. Then they would identify threats and threat categories. They would identify vulnerabilities and evaluate the potential risks. They would perform a site survey to evaluate the physical security controls and test existing systems and controls. The consultant would then evaluate the asset categories, threats, and vulnerabilities for security gaps. They would identify potential solutions to close those gaps and prevent criminal acts. The physical security report would look very similar to the IT security report in that recommendations would be prioritized and the design consultant would be able to provide cost estimates to implement recommendations as well.

The benefits to the organization of having both an IT assessment and a physical assessment when it comes to information protection are enormous. It offers options for protection solutions when one option may be cost prohibitive, another may be affordable. The combined assessment protects all information, not just electronic information or physical information. Most companies have both forms, whether they want to or not. The combined assessment may shed light on vulnerable areas that were originally thought to be well protected. The critical asset server room with costly locks and specialized temperature and atmospheric controls is seriously compromised by a hole in the wall covered by a mere cartoon.

Additionally, there is no shortage of motivation for criminals to go after critical assets. Attacks on protected information occur on a regular basis. Employees may make more money selling information they have access to than they ever would working in their regular job. Competitors may need your technology and are willing to interface with a third party to obtain it. The media may be interested in someone in particular for whom your organization has information. Terrorist and criminal groups are constantly searching for ways to compromise general business activities and cause harm to the economy. Corruption and crime is a reality, and private and public organizations need to do what they can to protect their assets and the information people have entrusted in them.

Physical Security

Physical security is also important in the protection of information for three main reasons. First, it can serve as multiple layers in protecting or guarding against inappropriate access to information. Proper physical security can secure the electronic devices on which the data is retained, thus preventing breach incidents. Servers, data drives, and mobile devices often contain protected information. Even if the intent is not to steal the data contained on a device the missing device may cause a business interruption.

Secondly, an organization cannot underestimate the sophistication of criminals and their ability to “crack the code.” Technology is advancing at an alarming pace and about the time the companies figure ways of securing their information, the criminals are developing the tools to get through the security. Although this is true for physical security as well, the

best solution is a combined IT and physical security approach to reduce the likelihood that an information breach will occur.

Lastly, most organizations have some form of physical information that they should protect. Despite our “green” efforts, much information still exists on paper or on portable equipment, such as drives or mobile technology. Some organizations may have information in the form of physical prototypes or research in progress that would be costly if it were exposed. In today’s increasing world focused on information and technology, the future success of a company or government organization could be solely hanging on its ability to keep it’s information private until which time it needs to share it. Physical security and protection of the information is critical to preventing a breach of the organization’s information.

The examples below are just a few physical security problems that security-consulting firm Business Protection Specialists, Inc. [7] has encountered that could have evolved into major security issues:

- An employee knew they would be leaving their company. Prior to giving notice, the employee broke into the human resource file cabinet and removed their signed nondisclosure agreement before leaving the company. The missing agreement was discovered only after the employee left to work for a competitor and now the company is less protected against the employee’s knowledge of company secrets.

- A company’s access control and alarm notification was not configured correctly. The employees did not know the system was not working as intended. The doors were left propped open and no alarm sounded after the requisite time lapsed. Later, company laptops containing sensitive information were stolen.

- BPS often comes across new clients that have poor access control or key control practices. Leadership may believe their facilities are secure, but if poor practices are followed in issuing cards or keys, maintaining the system, and collecting the cards or keys from exiting employees then the controls no longer exist. Former employees often have access to the buildings even years after leaving employment of those organizations.

- Even if the access control into the facility is appropriate, BPS routinely finds that areas containing sensitive information within a building are often left highly vulnerable. This is important because many information breaches are done by employees (who soon leave the company). BPS consultants were performing a site survey with a new client and were shown a series of filing cabinets that contained extremely sensitive documentation requiring high security. BPS briefly noted the lock cylinder on the cabinet and while touring a nearby department found a similar cabinet. The consultant easily located the key in a receptionist’s desk and went back to the area containing the highly confidential information. With the client watching, the consultant inserted the key and without resistance opened the cabinet with full access to the sensitive information.

IT security and physical security have the same goals when it comes to information protection. Working in conjunction, the appropriate security program will incorporate both tactics to provide a fail-safe method of protection. Additionally, both provide methods of

security that the other cannot. For a simple illustration, if a corporate laptop containing drawings, prototype information, or formulas is stolen, the release of data may be reduced if the laptop is properly encrypted. However, with today's sophisticated criminals and the advancement of technology, the company cannot be certain that the information breach has occurred once the laptop is out of their possession. If the data contains private information of customers, those customers may need to be informed that there was a potential breach of their information. Clearly, the best strategy is one that prevents the possible breach that would damage the organizations assets and its reputation.

There are best practices for keeping data secure is to ensure proper IT and physical security for your organization. The organization should identify critical information assets, as well as protected information of customers, users, or other outside parties in which the organization has an obligation to keep the information secure. The organization should then assess the protection of those assets and information. This could include performing a periodic third-party audits by an outside, or objective, organization to identify gaps in your security program and make recommendations to close those gaps. Frank Pisciotta, CSC, president and CEO of Business Protection Specialists, Inc., comments of the value of having the audit conducted by an outside organization:

> Typically organizations do not see the potential threats or vulnerabilities in their own security programs. Often a lack of incidents provides a false sense of security that security is effective, when in fact the organization is getting by on mere luck. Companies tend to act on security in a reactionary way. However, the best, and most effective security program is one that assesses potential future threats and protects itself against them."

A physical security consultant can assist you in the identification of gaps by performing a security audit on your facilities. This would entail looking at all facets of physical security, well beyond the door access and video surveillance systems you may have in place. People often override technical systems so procedures and policies are an important part of information protection as well. Post-it notes with passwords, shared passwords, unlocked file cabinets, papers left on desks overnight are just a few very minor samples of simple lapses in an organization's security program that typically occur on a routine basis. Consultants can help bring these issues to light, along with the major issues the organization may be overlooking and address them in a proactive way. A qualified consultant can also provide prioritization and cost estimates for solutions to closing the identified gaps.

Everyone wants to believe that the company's IT data is secure. A comic may hide the hole in the wall next to your servers, but the compromising of that data is surely nothing to laugh at.

References

1. http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-co... [8]
2. http://www.theemailadmin.com/2010/02/data-breeches-increase-legal-costs-... [9]
3. https://databreachcalculator.com/ [10]
4. http://www.informationshield.com/privacybreachcalc.html [11]

Author:
Frank Pisciotta
Featured Image:

Feature Technology

Related Sites from UBM Canon:

- Qmed - Qualified Medical Suppliers
- Medical Device + Diagnostic Industry
- European Medical Device Technology
- Medical Product Manufacturing News
- IVD Technology
- OrthoTec
- China Medical Device Manufacturer
- medtech*insider*
- medtech*insider* auf Deutsch
- Pharmaceutical & Medical Packaging News
- Pharmalive

Source URL: http://www.medicalelectronicsdesign.com/article/multilayer-information-protection-methods

Links:
[1] http://www.medicalelectronicsdesign.com/
[2] http://www.medicalelectronicsdesign.com/article/multilayer-information-protection-methods
[3] http://www.facebook.com/sharer.php
[4] http://www.medicalelectronicsdesign.com/department/feature
[5] http://www.medicalelectronicsdesign.com/categories/technology
[6] http://www.AltiusIT.com
[7] http://www.securingpeople.com
[8] http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_US
[9] http://www.theemailadmin.com/2010/02/data-breeches-increase-legal-costs-soar/
[10] https://databreachcalculator.com/
[11] http://www.informationshield.com/privacybreachcalc.html