

INFORMATION SECURITY SOURCE

REAL-WORLD TOPICS ON INFORMATION SECURITY AND YOUR COMPANY

INSIDE THIS ISSUE:

<i>Data Leakage Defined</i>	2
<i>Regulatory Corner - HIPAA</i>	2
<i>Simple Solution</i>	2
<i>Is the U.K. More Secure Than the U.S.?</i>	3
<i>Featured Breach</i>	3
<i>Control Point Message</i>	4

Why are Information Security issues so important?

- There are no shortage of Regulatory Compliance authorities, and yes, Big Brother is watching.
- Companies routinely overestimate the effects of their security efforts, creating a 'target rich' hacking environment.
- Laws fail to keep pace with rapidly-changing attacks.
- Internal staff can cause huge damage.
- Misunderstanding security issues can promote avoidance and foster a dangerous level of overconfidence..

INTRODUCTION

Control Point is a provider of information security solutions. We have extensive experience securing networks and their data for modest-sized businesses through Fortune 500 clients, State agencies, and the federal government, including the Department of Defense. We carry top industry and vendor certifications as well as being certified by the National Security Agency (NSA) to assess risk and make recommendations for remediation. Our approach is consultative. We gladly share



the benefit of our research with our clients to help them determine what recent industry changes would best fit them. We produce and distribute this newsletter to address security topics from a non-technical perspective. It is directed at decision-makers to aid in the daunting task of overseeing an ever-changing technical landscape. The opinions expressed herein are the results of our research, experience, observations, and intended to be beneficial. We welcome your comments!

INFORMATION SECURITY CONCEPTS FOR DECISION-MAKERS

- 1) **Do you have a formula that drives your budget for Information Security?** The basic rule is to completely assess your risks, decide what is not transferable (to insurance etc.), and determine a complete cost of risk. This value becomes your high water mark for your I.S. budget, thereby keeping you from spending more on security than the value of what you are trying to protect.
- 2) **Where do you get your updated security information from?** The answer can be somewhat difficult, depending on your structure. Do you depend solely on your internal staff? Have you considered a third party to share information with you? Are they informed and trustworthy? Do you periodically retain an outside firm to give you an unbiased report of your current security stance? The answer here is dictated by your organization's specifics. Consider all and choose wisely.
- 3) **Have you tasked Information Security (I.S.) to staff that lacks either the training, experience, or time to carry it out?** You wouldn't be alone. Too often management assumes that I.S. is an extension of I.T. and therefore should be lumped in with the



Courtesy of Google Images.

rest of the system maintenance responsibilities. There are several reasons why this does not normally work well in practice. At the very least, I.S. and I.T. tasks require different skill sets and checks and balances from one to the other.

- 4) **Simple is as simple does.** Don't fall into the lure of purchasing I.S. solutions based on their 'simplicity'. In-depth Security solutions can become quite complex and must evolve, even when using 'simple' equipment. Just think of what the solution is meant to protect and guard against.

TERM OF THE QUARTER - 'DATA LEAKAGE'

Improper data handling can undo a company as quick as any other form of breach...

Data Leakage is a broad term covering any undesirable OUT-BOUND transmission (or mishandling) of your critical data. Whether or not you already know the term, Data Leakage is a concept that is well worth becoming familiar with. EVERY organization is challenged with and has had problems in this area. Data Leakage involves personal, financial, or trade



Courtesy of Google Images

secret data, on clients, employees, your company, a partnership, or a current project.

Historically, a company would protect data by reinforcing the perimeter and monitoring the traffic flow for any 'recognized' malicious traffic. These are necessary steps, but they fall short when the problem is what authorized users are doing with the data. Improper data handling can undo a company as quick as any other form of breach; because isn't it the data we are trying to protect in the first place? If you are thinking, "I trust my employees completely.", consider this; whether intentional or not, attaching the wrong file to an email or saving something

confidential to a USB drive that is later misplaced, has the same result. Your company suffers the same regardless of the intent or method of Data Leakage.

The good news is, there are technologies to guard against the mishandling of data, even though you must give your employees access to critical data to do their jobs. Even in the case of an intruder penetrating your system, if they can't move the critical data out, all is not lost.

Not all Data Leakage solutions are created equal and we strongly advise engaging a trusted, knowledgeable consultant before committing to a product or solution.

Not only do the requirements cover data at rest AND in transit, they also address the Confidentiality, Integrity, and Availability (CIA) of the information.

REGULATORY CORNER - HIPAA

HIPAA compliance issues continue to pose challenges for the medical community, as well as non-healthcare entities charged with protecting patient data. Information Security solutions can directly support the Security and Privacy standards for information (data) under HIPAA. Not only do the requirements cover data at rest AND in transit, they also address the Confidentiality, Integrity, and Availability (CIA) of the information. Broadly speaking,

you must guard against, 1) unauthorized access or release, 2) alteration, and 3) deletion of the information.

This translates into a security solution that protects the information from intentional and inadvertent breach or release, invokes access and change controls, and institutes reliable backup solutions.

Another security requirement

can occur when using 3rd party vendors, e.g. billing entities, etc.. If the vendor has access to certain healthcare information, "...the 'covered entity' must require the 'business associate' implement appropriate security protections..."

Consulting an experienced Information Security provider can help simplify this process.



"Security tools come in a box; security solutions don't."

"WE NEED A SIMPLE SECURITY SOLUTION"

The title of this article brings to mind the old saying, "Be careful what you ask for..." We all want something to simplify our complex lives, of which I am no exception. But at the risk of sounding somewhat proverbial, there are certain things that will only yield what you put into them. An Information Security solution should top the list. Yes, I

have seen the marketing and product advertisements. They say again and again how simple, easy, automatic, etc., their products are. We even use some of these products in our solution delivery! It doesn't make the products bad, it just understates the level of expertise required to take complete advantage of their capabilities, and what more

may be needed. I recently saw a quote from VeriSign that made the point, "Security tools come in a box; security solutions don't." Security solutions are best designed by qualified professionals currently working in the field, and implemented with organizational buy-in..

IS THE U.K. MORE SECURITY CONSCIENCE THAN THE U.S.?

Is it the social tolerance for video cameras at every corner? The network of control rooms with staffs of people connected to all branches of law enforcement? Maybe it has to do with the European mindset that they are not so isolated as we Americans tend to think we are. Who knows for sure, but one thing is certain; in the world of digital systems the U.K. confronts and embraces information



security more readily that we do in the U.S. Some of our strongest standards were adopted from British Standards.

It isn't that we aren't aware of the potential for damage following a security incident. We just seem to apply the same rational to it as we do the likelihood of being involved in a car accident. We know it

can happen, but each morning we are all certain it won't be today. As little as four

years ago you could scarcely find a U.S. federal or state request for Information Security services. Commercial firms rarely considered bringing in outside security firms to validate internal efforts. Daily news reports confirm that assailants are having a field day as U.S. decision makers take a guarded approach to facing the need to preemptively and aggressively address their Information Security needs. On the bright side, we are collectively moving in the right direction, but those with much to lose should consider accelerated measures.

As little as four years ago you could scarcely find a U.S. federal or state request for Information Security services.

FEATURED BREACH - T.J. MAXX/MARSHALLS



The Story

C|NET reported the TJX Companies, which include T.J. Maxx and Marshalls clothing stores, suffered a system breach, resulting in as many as 45.5 million lost records. Protegrity states the loss to TJX Companies is currently estimated at \$1.6 Billion. In addition to personal data, the assailants obtained credit card data which was used to create fraudulent cards. These were in turn used to purchase gift cards from retailers like Sam's Club and Wal-Mart.

The loss to the banks issuing the credit cards and the retailers the gift cards were used at, is estimated at \$8 million.

The Breach

So how did this monstrous breach happen? Multiple sources throughout the security community (bonafide news reports, blogs, and hack chatter) put the blame on wireless connections that

were either poorly secured or not secured at all. This facilitated access to internal systems where the data was stored and/or transmitted between. There was also some mention of systems with less than desirable security that contained very sensitive data. The kicker is that this breach dates back to early 2003, with the credit card info believed to have been sifted from early to mid 2006 through early 2007!!

How many times have I heard, "We don't need help with our security because we have never been hacked." Right.

The Result

Aside from the numbers already quoted, C|NET reports that a major shareholder for TJX is filing a lawsuit claiming that TJX Companies wrongfully denied the shareholder access to the materials pertaining to the breach.

20/20 Hindsight Prevention

- 1) Starting with the obvious, secure the wireless or if encryption brings it to it's knees, don't transmit critical data over it!
- 2) Configure the internal network to withstand

peripheral areas of breach without losing critical data. In other words, if you store gold, make someone dig hard and deep before they can steal it!

- 3) Run periodic scans to expose vulnerabilities and patch them before they are compromised (PCI requirement).
- 4) Institute a Data Leakage solution. Even if the network was compromised this could have prevented the critical data from leaving the network, given the proper configuration.

Wrap Up

Given the information we have available to us, the use of standard Information Security best practices would have made this breach far more difficult to carry out. By instituting a few, well placed, advanced solutions, this breach could possibly have been prevented. At the very least, the duration of the compromise could have been reduced to hours or days, not months and years.

How many times have I heard, "We don't need help with our security because we have never been hacked." Right.

Marshalls.

At the very least the duration of the compromise could have been reduced to hours or days, not months and years.



2101 San Joaquin Hills Road
Newport Beach, CA 92660

Phone: 949-720-9233
Fax: 949-720-9232
Email:
services@controlpointis.com

Visit us on The Web!
www.controlpointis.com

Control Point is a proud reseller and service provider of the following:



Control Point maintains associations, certifications, and/or affiliations with the following organizations:



Control Point is an Information Security Solution Provider based in Newport Beach, CA. We have over 15 years experience securing data for commercial, state, and federal/ DOD clients. Our staff has extensive information system experience and have held government clearances as high as Top Secret (SCI). We carry nationally-recognized, top-level security certifications and work closely with our clients to provide security solutions that fit them. We also knowledge-share with your staff and can provide critical indicators to enhance their efforts.

CONTROL POINT MESSAGE

Choosing an Information Security Provider can number among one of the most critical decisions your company can make. When considering an outside provider, ask yourself the following:

- 1) Will they learn about us in order to provide solutions that are tailored to us?
- 2) Will they work well with our existing staff and contractors?
- 3) Are their people trustworthy?
- 4) Will they be receptive to our concerns?
- 5) Are they certified by reputable organizations?
- 6) Do they understand business concepts?



Lock down your data with the right Solution Provider!

- 7) Are they familiar with regulatory compliance?
- 8) Will they try to "over-sell" the solution?
- 9) How are their references?
- 10) What is their experience?

Your Information Security Solution Provider should be able to present you with sound information and choices so that YOU can make smart security decisions. They become your trusted advisors, and your second eyes on your systems. They guard your information as if it were their own.

We at Control Point believe strongly in this premise. Whether you decide to use us or another provider, we should all be subjected to the same scrutiny. It is your information. Guard it well!

Jim Cowden
(CISSP) (NSA IAM/IEM)
Chief Security Strategist

CONTROL POINT SERVICES

- Vulnerability/Risk Assessments
- Data Leakage Prevention
- Network Scanning Service
- Intrusion Detection/Prevention
- Security Appliance Managed Services
- Secure Remote Access
- Backup and Disaster Recovery
- Computer Forensics

HOW WE CAN HELP

Control Point conducts free information security reviews with interested organizations. These reviews help organizations identify security areas of need, as well as gain awareness of how new technologies can improve their security stance. Quite often the discussions reveal how to improve the business model/technology relationship.

Call 949-720-9233 to get started.