

**YOU'RE COMPLIANT, BUT ARE YOU PROTECTED?**  
Being PCI, HIPAA, SOX or NERC-CIP Compliant is No Protection When You Are Breached

A whitepaper from:

TDI  
1.800.695.1258  
info@tditx.com  
www.tditx.com



## **Being PCI, HIPAA, SOX or NERC-CIP Compliant is No Protection When You Are Breached**

Recently the country watched as Hannaford Brothers, a major grocery retailer in Maine, had to disclose its security had been breached by insiders who stole credit card information and caused millions of dollars in damages.

The chief counsel's office publicly stated: "We were hacked and credit cards for thousands of customers were stolen. We were 100% PCI DSS compliant."

Hannaford Brothers is now subject to millions of dollars in fines, litigation and is having to outsource its entire data center operations under extreme pressure.

But they were PCI compliant, met all the requirements and just passed an audit.

Experts said the breach should serve as a big lesson for retailers: It's as important to limit the network access of employees and regularly monitor system activity as it is to purchase security technology to block attacks from the outside. Furthermore, it's foolish for a company to consider itself bulletproof because they achieved PCI DSS compliance, as Hannaford's claims it did.

"The overarching conclusion I have that keeps getting reinforced is that the low-hanging fruit is inside the company and insiders are always getting more network privileges," said Mark MacAuley, a York, Maine-based IT security consultant who shops at Hannaford's regularly. "I don't see how anyone at Hannaford could get that level of access unless they were a very well-known entity."

SearchSecurity.com March 2008

Every major regulatory rule mandates that a firm must protect its confidential data—credit card, patient record, corporate confidential information from undocumented intrusion. You can be 100% compliant with the rules of Sarbanes Oxley but if your insider has unfettered, unlogged and uncontrolled access to the infrastructure, they can steal confidential data, sell it on the internet and your company is out of business or liable for fines which may drive it out of business. Impact to customer confidence alone can destroy a brand which took years and millions to build.

The dirty little secret is that all existing log management systems and security systems were built for the previous generation of technology where there were no virtualized systems, there were no service processors and insiders were your most trusted people. They were built to watch the outside intruder – not the activity of the insider.

Welcome to the new world of cyber intrusion. Insider attacks which result in theft of confidential information for personal gain, financial gain or employee retribution can result in datacenter disruption, loss of information and major compliance headaches.

Today's compliance demands that confidential data must be protected:

- **At all times**
- **In all machine states**
- **In all environments**
- **At all access points**
- **Even from insider intrusion**

## ***At All Times***

---

“At all times” means that credit card or patient data must be protected 100% of the time, not just when the O/S, network or hypervisor is up, healthy and running properly. What about the times when the O/S is down? What about the times your trusted employee is installing a configuration change or patch? Who is watching the system then? Did they do what they were supposed to do or are you left with a bit of “extra” code, a special patch or other backdoor impact which leaves gaping holes in your security and exposing confidential information?

This is not your logging system or traditional security system. All existing logging and security systems are completely blind when the network, O/S or hypervisor is not operational. Yet that is just the time the clever criminal strikes. You were compliant, but you are now subject to huge fines and litigation.

## ***In All Machine States***

---

The network is fine and the O/S is working. But the authorized user puts the machine into a “single state” to apply a security patch. Who is watching the machine in “single state?” Not your log management system or your traditional security system.

They are completely blind to single state access because they cannot see below the network level in the technology stack. In fact they require the network and operating system to be functioning properly – they rely on the very environment they are trying to protect.

## ***In All Environments***

---

Why have a log management system that cannot protect your virtualized systems? Why have one log management system for Windows, another for Linux and still another for industrial control devices? Having this many devices managing your center opens the door to intrusion because tracking intrusion consistently across multiple environments can be very difficult.

Traditional log management systems do not monitor virtualization, the single largest technology trend in the last three years. Many firms will have 30%-60% of their systems virtualized in the next two years. Yet, their logging systems cannot see the underlying virtualized infrastructure because they can not be installed on the hypervisor without voiding it's warranty and performance guarantees.

## ***Across All Devices***

---

All devices must be logged, audited and secured at all times in all environments.

Are you aware that your network can be accessed via a printer port or through a router or switch? In May, 2008, the FBI reported that the Chinese government used Cisco routers to break into U.S. corporate and government networks.

## ***Protect All Access Points***

---

SANS Institute, the world's most respected IT security and audit training organization recently recognized the intrusion threat from the Baseboard Management Controller (BMC) which are now shipped on every computer, router or switch. These constitute a separate computer within a computer that is completely unprotected by today's log management systems or security systems. The U.S. government has determined there are growing hacks of both government and corporate computers via the BMC. You may be SOX compliant or PCI compliant, but if you are hacked through the BMC, you can have the same problems as Hannaford Brothers (see attached).

## ***More Information***

---

TDI has more information on this subject and would welcome a conversation with you and your security staff to discuss in detail how the BMC, ILO, service processor and other points of entry into your IT infrastructure can be exploited. Once exploited they are used to gain entry into your environment and remove critical confidential information by not only the outside hacker – but the inside thief as well!

To engage in a technical demonstration, a live demonstration, address configuration or pricing questions, please call 1-800-695-1258 today or visit our web site at <http://www.TDItx.com/>.

## **About TDI**

---

### **What We Do:**

For 15 years TDI pioneered, patented, developed and deployed a family of technologies based on the "outside-in" infrastructure management paradigm for failure-intolerant customers such as The National Security Agency, The United States Army, Bank of America, Pfizer, Verizon, and the European Space Agency. TDI has over 280 customers with 3,200 installations.

### **How We Are Different:**

The "outside-in" or "out-of-band" infrastructure management paradigm is not dependent on the infrastructure it is managing. If the O/S or hypervisor goes down, TDI still manages, monitors, finds the root problem cause and remediates the problem - all from a web browser. Virtualization and the advent of the baseboard management controller (BMC) have created a new paradigm for security, logging and event management that makes previous agent-based, polling technologies obsolete.

### **Why This Matters:**

Whether it is virtualization, log management, or infrastructure management, the world is moving to a "self-healing" infrastructure. Human intervention is too expensive and prone to risk.

To heal, one must diagnose. To diagnose, one must see what is going on both at the lowest level of the device, and from a top down "holistic" perspective. With the advent of CIMOMs everywhere, a functional Alert Standards Format and SMASH deployment, TDI's technologies capture and interpret the data most relevant to healing a problem before it takes down the infrastructure.

TDI is located in Plano, Texas and has 40 employees. The company receives no venture funding and is profitable and growing. In each of the previous 3 years, TDI has been recognized as one of the Deloitte Fast 50 high tech firms in the region.

### **TDI Headquarters**

1600 10th Street, Suite B  
Plano, Texas 75074  
(972) 881-1553  
(972) 424-9181 (fax)  
[www.tditx.com](http://www.tditx.com)

**Copyrights and Trademarks**

Copyright 2008 TDI

All Rights Reserved. This material is subject to copyright protection.

All other trademarks are acknowledged as the property of their respective owners.

This document and the products to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of this document or of the associated products may be reproduced in any form by any means without prior written authorization of TDI.

MATERIAL IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.



TDI  
1600 10th Street, Suite B  
Plano, TX 75074  
1.800.695.1258

# Malware cited in supermarket data breach

Malware cited in supermarket data breach

By JERRY HARKAVY, Associated Press Writer Fri Mar 28, 4:28 PM ET

PORTLAND, Maine - Unauthorized software that was secretly installed on servers in Hannaford Bros. Co.'s supermarkets across the Northeast and in Florida enabled the massive data breach that compromised up to 4.2 million credit and debit cards, the company said Friday.

The Scarborough, Maine-based grocer confirmed a report in The Boston Globe that it told Massachusetts regulators this week about the link between the breach and the illicit programs, known as "malware."

The company doesn't know how the malware — short for malicious software — got onto nearly all its 271 stores' servers, Hannaford spokeswoman Carol Eleazer said.

"Virtually everything is possible," she said. "There are still many, many aspects that we don't totally understand." At least 1,800 cases of fraud have been linked to the data breach, with unauthorized charges showing up as far afield as Mexico, Italy and Bulgaria.

The breach has prompted concern in the industry because it appeared to be the first large-scale theft of credit and debit card numbers while the information was in transit.

The usual mode of attack targets data sitting in databases, as in the record-setting theft of information from Massachusetts-based TJX Cos. involving least 45 million card numbers belonging to customers of T.J. Maxx and Marshalls stores.

TJX Cos. agreed to regular external security audits in a settlement this week with the Federal Trade Commission regarding the breach, which occurred in 2005 and 2006. The FTC lacks the authority to impose fines.

Sherry Lang, TJX's senior vice president for investor and public relations, said the company disagreed with the FTC's allegations that it didn't properly protect customer data. But she said the settlement "is consistent with the agreements between the FTC and other retailers that have been victimized by cyber crime." A federal consumer lawsuit against TJX is pending in Boston.

Hannaford has said its breach, which occurred between Dec. 7 and March 10, allowed credit and debit card numbers to be stolen as shoppers swiped their cards at checkout line machines and the information was transmitted to banks for approval.

The malware turned up in all Hannaford stores in New England and New York and in most of the company's affiliated Sweetbay stores in Florida, Eleazer said.

The finding was revealed in a letter from Hannaford general counsel Emily Dickinson to Massachusetts Attorney General Martha Coakley and Gov. Deval Patrick's Office of Consumer Affairs and Business Regulation.

Eleazer declined to release a copy.

In Maine, Assistant Attorney General Linda Conti — who said she spoke with investigators — said the breach began as a single message sent to a single location that was then sent to multiple locations. She declined to discuss specifics.

Conti said her office is investigating whether the company did everything in its power to protect consumers.

Data from swiped cards would flow from the cash register to the store server, then perhaps to a regional server before being transmitted to a credit center for approval, said Avivah Litan, security analyst at Gartner Inc.

"It sounds like they were snooping on that traffic with malware," she said.

The involvement of the software had not been previously disclosed "because of the confidential nature of the investigation," Eleazer said. The breach remains under investigation by the U.S. Secret Service.

Even while the Hannaford hack was still going on last month, the company was found to be in compliance with security standards required by the Payment Card Industry, a coalition founded by credit card companies.