Volume 4 - Issue 7 July 2012

The Franchise Valuations Reporter

Franchise Technology Risk Management

Hot Off the Presses

The third edition of my BNA Tax Management Portfolio, "Tax Aspects of Franchising," has just been published. To purchase a copy, contact our office.

Also, we are proud to announce the publication of the following:

"Current Damages Issues in Franchise Disputes" appearing in the June issue of Dunn on Damages; and

"Canada's Tim Hortons Case: Lessons Learned About Franchisors' Rights, Class Action Certification and Rules of Expert Testimony" a white paper co-authored with Ned Levitt and published by CCH Business Franchise Guide a few weeks ago.

Bruce S. Schaeffer, Editor
Bruce@FranchiseValuations.com
212.689.0400

Our Expertise

Within the franchise, distribution and dealership context, we are experts in:

- Damages, Valuations & Expert Testimony
- Finance, Accounting and Tax
- Cyber Security and E-discovery of Electronically Stored Information

We offer a free initial consultation. If any readers have questions, you are welcome to email or phone us and we will provide our best answer as quickly as possible.

Special Edition on Penetration Testing and Cyber Security

In this issue we focus on cyber security issues that affect franchises. The announcement by the Federal Trade Commission that it had filed a complaint against hotel franchisor, Wyndham Worldwide, for failure to protect consumers' personal information triggered a feeling of déjà vu among Franchise Valuation's network security experts. *Haven't we seen this movie before?*

At the risk of sounding like Cassandra, we went back to the newsletter archives and selected a few stories that we thought our readers would find instructive. Whether or not the FTC prevails, the message to franchisors and their advisors is clear: Take steps now and avoid becoming another Wyndham.

What Wyndham Complaint Says to Franchisors

FTC Complaint Raises the Stakes

On June 26, 2012, the Federal Trade Commission filed a complaint in U.S. District Court for the District of Arizona seeking an injunction against Wyndham Worldwide Corp and three of its subsidiaries, one of which is the franchisor of such prominent hotel brands as Ramada, Howard Johnson and Days Inn.

The FTC charged that Wyndham failed to take security measures against known security vulnerabilities, failed to follow proper incident response procedures, and misrepresented in public statements what security measures it had taken. The phrase "known security vulnerabilities" is an understatement. The complaint cites three separate security breaches of the company's data center in less than two years.

While Wyndham officially disputes many of the claims against it, some franchisees have publicly stated that they have been warning of security weaknesses for years. There are widespread implications in this case for the franchise community and franchise companies that continue to ignore them will be doing so at their own real peril:

1. Attacks Are Ongoing.
Lightening does strike twice or even three times. And it's not random. Symantec notes "a rising tide of advanced target attacks in 2011. . . It is possible that smaller companies are now being targeted as a stepping stone to a larger organization because they may be in the partner ecosystem and less well-defended." This is exactly how intruders first gained access to the Wyndham corporate network. **(See "Hackers Zero In On Small Firms," from our August 2011 issue; and "Cybercriminals Using Franchisee-First Strategy," from our May 2011 issue, below.)**

2. Attacks Are Predictable.
Cyber attacks generally follow three steps, according to our network security expert, Henry Chan:

I. Breach the perimeter through
   a. Human vulnerabilities or

Bruce S. Schaeffer, Editor
Bruce@FranchiseValuations.com
212.689.0400

Franchise Technology Risk Management

Our franchise law and computer forensics experts provide consulting and implementation of all aspects of cyber security, ESI management and e-discovery for franchise systems - from preparation of cyber security and ESI-related policies and procedures manuals through collection, preservation, processing, production and presentation.

To inquire about our services, please e-mail
Henry@FTRM.biz
or call (212) 689-0400

Worth Reading

We recommend this fascinating *Washington Post* series on cyber security for an explanation of "Zero Day" flaws**.**

Part I: Understanding Cyberspace Is Key To Defending Against Digital Attacks

Part II: Cybersearch Engine Shodan Exposes Vulnerabilities

DISCLAIMER

The information provided in this newsletter is for informational purposes only and should not be construed as legal or expert advice which can only be obtained from appropriate professionals. Franchise Valuations, Ltd. and Franchise Technology Risk Management provide such expert advice on the topics addressed herein.

Please visit our websites at
www.FranchiseValuations.com
and
www.ftrm.biz

b. Application vulnerabilities
II. Obtain privileged access by becoming an authorized user; then
III. Exfiltrate the information

Note the part about "human vulnerabilities." *Social networks are replacing e-mail as the preferred intrusion vector.* Security is not just a technology issue. People are the weakest link.

3. The Consequences Are Ghastly.
A network breach opens a franchise up to all kinds of massive problems, including:

- Loss of trade secrets
- Direct costs to repair and fortify the network against future threats
- Costs in penalties, crisis management, and regulatory compliance
- Loss of reputation and customer loyalty

A Ponemon Institute study examined 49 U.S. companies that had been hacked and found the average per capita cost of a breach was $194 and the average incident cost $5.5 million.

The Wyndham complaint also demonstrates that the FTC can no longer be considered a sleeping dog.

4. The Time For Action is Now.
Implementing a list of 10 best practices for network security is no substitute for a comprehensive approach, but it is a start. **(See "Penetration Testing: Why Franchise Systems Need Information Security," available here.)**

The information security team at Franchise Technology Risk Management provides penetration testing, cyber security analysis, and consulting services for the franchise, distributorship and dealership community. For an initial consultation on your cyber security needs, please contact us.

Hackers Zero In On Small Firms

Unsuspecting Business Owners Pay Steep Price for Complacency

A front-page article in *The Wall Street Journal* highlighted an increasingly tantalizing target of Internet hackers: small companies. Among the victims examined in the article: a newsstand, a burger restaurant, a pizza parlor and a Ford dealership. While the media tend to report extensively on cyber attacks against large companies (Sony PlayStation, Citibank, Lockheed Martin), any retailer that accepts credit or debit card payments or uses online banking is equally vulnerable.

Franchise outlets are particularly inviting to those seeking customer account details because owners tend to be unsophisticated about basic hacking precautions. The WSJ report cites a 2010 survey conducted by the National Retail Federation and First Data Corp. which found that 64% of small- and medium-sized business owners believed they weren't exposed to card data theft and only 49% had conducted an assessment of their security.

Whether the breach is from a disgruntled employee or from a criminal conducting a remote electronic sweep, hackers have declared open season on small businesses. Owner/victims interviewed for the WSJ report were shocked to discover that complying with the card-issuers' standards (PCI-DSS) did not provide sufficient protection. In addition to having to cope with the general business disruption caused by an unauthorized intrusion, some were hit with tens of thousands of dollars in fees for post-incident forensic security examinations. For a business operating on thin margins, one attack can be a severe setback.

Cybercriminals Using Franchisee-First Strategy

Security Experts Recommend Amending Franchise Agreements and Operating Manuals

According to an article in *Multi-Unit Franchisee*, the use of a "franchisee-first attack" strategy by hackers to penetrate computer systems is becoming a common scenario. Frequently, the first successful breach occurs at a franchise location and then spreads to the whole corporate system; thus, penetration of one franchise unit's security can give hacker gangs a master key to the entire network. For a restaurant chain, a single report of credit card data loss can have the same negative impact as a food safety failure. A single incident can wreck the reputation of the entire system, cost millions to clean up and expose the chain to litigation for years to come.

Lately we've noticed more coverage of this issue than usual, not just in the general media, but particularly in the franchise media (*PizzaMarketplace.com, Multi-Unit Franchisee, Nation's Restaurant News*). You would think that by now franchise systems would have acted to mitigate their security risks but apparently that's not the case. In our experience we know of less than a handful of franchise companies that engage in any, much less regular, penetration testing.

PizzaMarketplace.com, citing *USA Today*, says that because hotels (which gained notoriety for hacker attacks in recent years) have taken steps to harden their networks (other than Wyndham), thieves are now going after the low-hanging fruit - restaurants. Other favored targets of hackers trying to steal payment card information are clothing and sporting goods chains.

And franchise systems should further be aware that the growth in the use of mobile devices such as tablets and smartphones to process orders and payments has introduced new access points for data thieves. In an attempt to reduce identity theft incidents through these and other devices, the major credit card issuers have tightened rules for merchants with the latest version of the Payment Card Industry Data Security Standard (PCI DSS v2.0), which is mandatory for vendors accepting credit or debit cards, and became effective on January 1, 2011.

Franchise systems must review their situations. A good starting point is Visa's Payment System Security Best Practices for Franchises which includes the following areas: (1) Payment Application Security; (2) Network Security; (3) Remote Management Application Security; (4) Franchisee Contractual Agreements; and (5) Communication and Training.

If techie talk makes your eyes glaze over, at least pay attention to the last two points by amending your franchise agreement or operating manual to include data security policies and mandating ongoing security awareness training. Franchise Technology Risk Management, the technology division of Franchise Valuations, Ltd., specializes in implementation of proper technical and written procedures for franchise systems. Contact us for more information.

Top Cyber Security Risks

Cyber Attackers on the Prowl for Loosely Guarded Networks

(One of our articles from July 2011)

First, hackers brought down the CIA website; then Citibank and the IMF announced they were hacked; and the US declared that a cyberattack will be considered an act of war to which we may respond with "a missile down your smokestack."

On average there has been at least one cyber event per day since 2006, and it is not just major banks or government agencies that are compromised. These new sophisticated attacks can be launched upon any company but especially those with major global brands that serve millions of people on a daily basis. Previously, a series of DDOS (distributed denial of service) attacks were successfully used against Visa, Mastercard and PayPal. On June 14, 2011, the Federal Reserve was reported as a possible target of attack, then it was Sony that was overwhelmed with Internet traffic.

The unfortunate common theme among these recent attacks is the lack of proper penetration testing and software patching for known vulnerabilities in third party software such as Adobe's PDF file format regularly used in targeted spear-phishing email campaigns.