Tech Firms Face a Wide Range of Security Challenges

For today's tech companies, protecting intellectual property, sensitive information and electronics have become increasingly difficult as threats from hackers, identity thieves, corporate spies and freight hijackers become more sophisticated. In response, tech companies have poured millions of dollars into beefing up IT security at their firms[1]. However, a short-sighted focus on high tech security solutions can leave tech companies even more vulnerable. Only by hiring well-trained, professional security officers can tech firms achieve true security.

Threats to Intellectual Property

One of a tech company's most valuable assets is its intellectual property, an attractive target for hackers, ratings-driven tech publications and corporate competitors.

That's why IT departments industrywide spend countless hours and millions of dollars thwarting digital attackers. They set up and utilize firewalls, anti-ping devices, data encryption systems, complex passwords and virus protection software. Often though, thieves don't gain illicit access by breaking through a firewall or implanting a Trojan horse virus. They come right in through the front door. The following facts illustrate the seriousness of the problem:

- According to the U.S. Commerce Department, intellectual property theft is estimated to top $250 billion annually.[2]
- In 2008, former San Jose computer network administrator Andrew Madrid posed as a security guard and IT employee to gain access to several Silicon Valley companies, stealing computer[3] and IT equipment.[4]
- The chief of operations at First Base Technologies, an ethical hacking firm, posed as a visitor to gain access to a tech client's computers. He was able to obtain a voice mail guide with default passwords, information about spending on advertising, bank statements, a staff directory and information about corporate strategy.[5]

Identity Theft

As identity theft becomes an increasingly prominent issue, another major area of concern for tech companies is the protection of customer, employee and client information. Housing millions of electronic records, tech companies are an attractive target for criminals. Although sophisticated hacking is certainly a real threat, tech companies also need to maintain effective protection from simpler attacks. Tech firms have good reason to be concerned:

- Javelin Strategy and Research Center, a market and consumer research firm, reports that cases of identity theft rose 12 percent in 2009.[6]
- Low-tech methods for stealing personal data are still the most popular for identity thieves, with stolen wallets and physical documents accounting for 43 percent of all incidents.[7]
- On Feb. 18, 2010, thieves broke into Arrow Electronics, a Fortune 500 electronics distributor[8], and stole a laptop containing more than 4,000 employee records. According to news reports, the personal information stolen included names, addresses, telephone numbers, Social Security numbers, and credit card information.[9]

1 Hardware to Drive IT Spending Growth in 2010, *Network World*, April 13, 2010.
2 How to Avoid Intellectual Property Theft, CIO.com, July 10, 2006.
3 Ex-computer network administrator faces 12 years in prison for string of tech crimes, *San Jose Mercury News*, November 10, 2008.
4 Drug Dealing Sysadmin Cops to Hacking and Burglary Offences, *The Register* (UK), November 13, 2008.
5 How to Spot – and Stop — a Spy, *ComputerWorld*, April 14, 2008.
6 Identity Fraud is At an All Time High, PRNewswire, February 10, 2010.
7 Identity Theft Statistics – Reason For Concern, Antivirus Administrator, April 12, 2010.
8 About Arrow Electronics, http://www.arrow.com/about_arrow/index.html
9 Arrow Electronics notifies 4,004 employees of stolen laptop, DataBreaches.Net, June 22, 2010.

Cargo Theft

Trailers, warehouses and distribution centers full of expensive computers, hardware and other high-end electronics are an alluring target for criminals. Large-scale, high-value[10] cargo heists accounted for tens of millions of dollars in losses last year.[11] Consider the following:

- A study conducted by FreightWatch International found the electronics industry suffered a higher number of cargo theft incidents [12] than any other sector last year, with robberies increasing by more than 12 percent[13].

- In January 2007, an alert security officer in Fort Worth, Texas, foiled a plot to steal at least two full trailers of electronics from an LG Electronics warehouse[14]. After failing to hear from his partner, who had been tied up in a truck, the officer arrived on the scene and spotted the robbers trying to hook up the trailers. They fled, leaving behind the two trucks.[15]

- At a computer logistics company warehouse in Los Angeles, cargo thieves broke in, set off the main security system and disabled the backup before leaving. When police arrived six minutes later, they thought it was a false alarm and left. The thieves simply waited three hours until the coast was clear, returned, and stole $4.5 million worth of electronics.[16]

- In February 2006, cargo thieves took advantage of a bathroom break by a driver at Ampro Systems in Fremont, Calif., to steal $200,000 in flash memory cards from a delivery truck. [17]

For Tech Firms, Protection of Intellectual Property, Customer Records and Electronics Inventory Requires Reliable Officer-Centered Security

To deter hackers, thieves and spies, tech companies must employ effective integrated security solutions, including the use of competent, well-trained security officers in charge of monitoring and patrolling facilities, controlling building access and guarding company property.

> *"It took less than nine seconds for an unauthorized visitor to take over an entire computer network, erase the primary and secondary databases, and plant a Trojan horse program."*[18]
>
> **Joseph Ricci**
> CEO of Ricci Communications

> *Cargo thieves will get an "order" for, say, Sony digital cameras or Dell laptop computers… The bandits will go to the manufacturer's distribution center, conduct surveillance using binoculars and watch the loading docks and trucks come and go. "After a few days, it doesn't take much to figure which trucks are moving which products. Then they will follow a truck that leaves late in the afternoon knowing the driver will stop in a few hours to eat dinner."*[19]
>
> **Lt. Ed Petow**
> 28-year veteran of the Miami-Dade police force
> (as reported in *Shipping Digest*)

10 U.S. Cargo Theft: A 2009 Review, *FreightWatch International*, January 29, 2010. Pp. 5
11 Ibid. Pp. 2
12 U.S. Cargo Theft: A 2009 Review, *FreightWatch International*, January 29, 2010. Pp. 1
13 Ibid. Pp. 1
14 Suspicious Guard Foils Huge Electronics Heist, *Fort Worth Star-Telegram*, January 9, 2007.
15 Suspicious Guard Foils Huge Electronics Heist, *Fort Worth Star-Telegram*, January 9, 2007.
16 Increase in Cargo Theft Has Caught Law Enforcements Attention, Fleet Owner, September 1, 2009.
17 Thieves Target Tech Firms, Trucks Hit at Lights, On Loading Docks, *San Jose Mercury News*, July 28, 2006.
18 Uniformed Protection: A Low-Tech Approach To Tech Security, SecuritySolutions.com, February 1, 2003. http://securitysolutions.com/mag/security_uniformed_protection_lowtech/
19 Cargo crime buster turns 10: TAPA rips down walls between corporate security and logistics, *Shipping Digest*, April 30, 2007.