Taking the Fight to Fraud

“Know thy self, know thy enemy. A thousand battles, a thousand victories.”

– Sun Tzu

The Chinese general, Sun Tzu, knew nothing of the threats posed by fraud upon modern-day businesses. But he was keenly aware that the first step in defeating his enemies was to understand their strengths and weaknesses – and those of his own.

The strength of fraud’s impact on business is clear:

- 60 percent of companies were affected by fraud in the past year *
- 1.1 percent of revenue is lost to fraudulent activities *
- Percentage of US companies describing themselves as highly or moderately vulnerable to the following frauds: *
  - Information theft (33%)
  - Theft of physical assets (20%)
  - Management conflict of interest (25%)
  - Vendor, supplier, or procurement fraud (27%)
- More than 286 million unique variations of malicious software currently exist. Less than a decade ago there were only 60,000. **

* Kroll Advisory Solutions’ 2012 Global Fraud Report
** Symantec's Internet Security Threat Report, April 2011

The weaknesses exposed by today’s fraudsters are due, in large part, to the accessibility of critically important business data. Such as the financial data that drives your day-to-day operations and long-term investments. And the intellectual property that helps you create a competitive edge. And the transaction records your clients trust to be kept confidential and safe from unauthorized intruders. How well you safeguard these valuable resources can, and will, impact the reputation and success of your business.

Know Thy Enemy

Unlike conventional enemies, fraud is often a faceless threat. And it continues to morph into different forms:

- IT-related – Includes hackers, email scams, phishing, vishing, trojans, keyloggers, malware, spyware, adware, bots, viruses, and worms.
- Check fraud – Ranges from counterfeit checks and altered checks to forged signatures.
- Wire fraud – Unauthorized individuals performing wire transfers to fraudulent accounts.
- ACH debit fraud – Transactions are initiated or altered to misdirect or misappropriate funds.
Know Thy Self
According to Kroll Advisory Solutions’ 2012 Global Fraud Report, the biggest fraud threat that corporations face comes from within. Of the 839 senior executives polled, two-thirds responded that their companies were hit by fraud in the past year – and inside perpetrators were the key suspects.

Why? Again, the Kroll Report sites the easy access to confidential information by employees, agents, and other company representatives. And with the proliferation of laptops, smart phones, flash drives and other mobile devices, confidential data is as close as your pocket and briefcase.

But it can also be attributed to a simple lack of awareness. While much of the fraud that occurs is initiated internally, the greater perception is that external forces are to blame and that’s where a greater focus on protection lies.

Fighting Back
Because the threat of fraud comes from within and without, companies must take a multi-layered approach to fighting back. In many cases, technology has kept up with fraud, providing software, hardware and cash-management solutions that can dramatically improve protection levels. But many of those solutions come with associated costs.

Fortunately, there are processes and procedures you can implement today that can help greatly reduce your exposure to fraud with little or no impact on your bottom line.

Dual Control Procedures
This procedure requires the active involvement of two people with separate duties. Each is required to perform a specific task before authorizing such activities as making online payments or purchases, processing payroll, or accessing sensitive corporate data. Alternating employees into and out of dual control positions can help assure an even greater level of internal security.

Laptops and Mobile Device Security
Protect laptops, tablets, smart phones and other mobile devices with a startup password so that data is inaccessible if the devices are stolen. Delete old e-mails, text messages, call logs and unwanted files from all portable devices. And whenever available, take advantage of a device’s built-in encryption capabilities and password protection features.

Fraud Awareness Programs
Threats continue to change; therefore you need to provide employees with information to help reduce their exposure to fraud. Teach employees how to identify potential attacks such as phishing and vishing scams, and malware threats that can infect individual computers and entire networks.

Employee Theft Prevention Programs
Provisioning procedures should be in place to help administer the distribution of sensitive equipment and access to important data. Some software solutions can instantly grant, revoke or modify access to any operating system, application, web portal or other IT assets without manual intervention.

Scrutinize Account Balances
Review your account balances on a daily basis to identify potential fraudulent transactions as soon as possible. Left unchecked, accounts can be repeatedly accessed over the course of days, weeks, or months, draining your financial resources and making remediation efforts more complicated.
The battle against fraud is not one that has a definitive ending. Threats – both internal and external – will always be present and will continue to become more malicious and effective. Instituting sound policies and procedures can help you protect your company’s most valuable assets.

In the next edition of *Treasury at a Glance*, we’ll take a look at some of the technologies available to help in the fight against fraud.

For more information on how you can prevent fraud, contact your Relationship Manager or Treasury Management Representative. [www.53.com/riskmanagement](http://www.53.com/riskmanagement)

The security information in this article is based on best practices that should be brought to the attention of your employees. **THIS INFORMATION DOES NOT ADDRESS ALL SECURITY RISKS AND BEST PRACTICES AND THEREFORE SHOULD NOT BE USED AS A SOLE MEANS OF SECURITY TRAINING FOR YOUR EMPLOYEES.** Work with your technical resources to add discussion points about security issues, policies and practices specific to your company or function within your company. That way, your employees will recognize the role they play in protecting your organization.

Articles contained herein are reprinted with permission.