

# LTD & ASSOCIATES INC.

Volume 2, Issue 1  
May 2003

## NEWS & VIEWS

Welcome to the second edition of our quarterly newsletter. From the feedback we received following the first edition release, it appears that our goal of keeping you our readers and clients abreast of current security and investigative issues, was met with overwhelming success.

Remember to sign up on line through the LTD & Associates Inc. website to make sure that you are notified automatically when subsequent newsletters are sent out.

Again thank you for your support.



### ***Inside this issue:***

Linc Fit-Laptop Security	2
Crisis Management	2
Business Continuity Plan	2
Investment Schemes	3
Identity Theft	3
Employee Screening	3
Intellectual Property	6

### **Special points of interest:**

- Organizations with Fraud Hotlines cut their losses by 50%.
- Small businesses are the most vulnerable to fraud abuse, the average loss is around 100K.
- Fraud losses caused by persons older than 60 are 27 times higher than losses caused by employees 25 years and younger.
- The average internal fraud scheme lasts 18 months before being detected.

## LOSS PREVENTION-A GUIDE TO VIGILANCE

It's not something most business owners or managers like to think about, but when it comes to loss prevention, one of the biggest dangers can be your employees. Statistics reveal that about 9% of the average company's stock is stolen by employees every year. Employees can steal everything from pens, paper and light bulbs to maintenance tools, computers and of course, retail stock. Consider the following "Loss PreventionTips" to help eliminate this serious problem: Keep detailed inventories of everything, Institute a Loss Prevention Plan, Know your employees to detect signs of financial or other problems, Do thorough background checks of all prospective employees, Insure your equipment against theft, Consider having high-risk employees bonded. Source Bellzinc and Richard Skinulis.

## LINC FIT – LAPTOP SECURITY DEVICE

The theft of Laptop computers and other audio visual devices continues to be on the increase worldwide. Not only is the cost of replacing this equipment expensive, time consuming and bothersome, it's the potential for information and technology loss which can be the bigger issue. A new product has just hit the marketplace which is endorsed by LTD & Associates and we are the only security company to have exclusive "dealer status" with the manufacturer.

"Linc Fit" a furniture based product, is designed to not only help stop Laptop theft but it also functions as a clever desk top wire manager. Designed to work with existing security cables, "Linc Fit" with it's patented security locking ring, doubly secures your Laptop making it harder for thieves to steal. Additionally, "Linc Fit" virtually eliminates the problem of having wires and cables scattered all over your work surface. Using the wire manager which is located inside the "Linc Fit" your security cable, power source, internet connection, telephone lines are all neatly tucked away below the desk surface, but remain easily accessible when you need them at desk height. According to the Computer Security Institute it is estimated that 97% of stolen computers are never recovered and that 620,000 computers were stolen in 2002, this is not a very reassuring picture.

For a demonstration on how "Linc Fit" can work for you in protecting your equipment and technology, contact LTD & Associates Inc.



Protecting Your Equipment & Technology

## CRISIS MANAGEMENT – WORKING TOGETHER

The heightened risk of terrorist threats and the equally unpredictable natural disasters, underscores the critical importance of effective crisis and business continuity planning. Crisis management has become an increasingly important aspect of modern business management, linking the functions of risk management, business continuity, security, emergency response and recovery. Under traditional emergency management models, the government's first responsibility is public safety. Economic disruption to business and the economy has been considered a private-sector issue. The private sector, for example, owns a high percentage of the national infrastructure, power, water, telecommunications and financial services. The overlap between public (government) and private sectors responsibilities requires a new approach to crisis management and business continuity integration. To develop a symbiotic relationship between public and private organizations, it is essential to form a community line of attack when preparing a crisis management strategy. Initially, all organizations must identify the most critical members of their community. This should include partners and customers, as well as Federal, Provincial and Municipal entities. Source CPA.

*Organizations that do not have access to updated emergency information through personal relationships, are hindered in their ability to adequately respond to a crisis.*

## ESSENTIAL INGREDIENTS OF A BUSINESS CONTINUITY PLAN

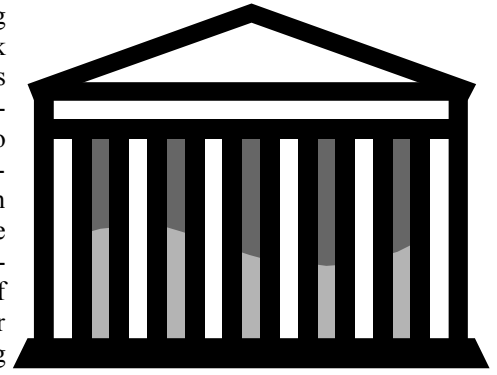
- 1 – Senior management support secured.
- 2 – Definition of plan scope business units and project teams.
- 3 – Completion of risk assessment, response, recovery and restoration strategies.
- 4 – Include security procedures with business continuity plan.
- 5 – Information backup, storage and recovery procedures.
- 6 – Identification of critical dependencies both internal and external.
- 7 – Verification of business continuity plan with third party suppliers.
- 8 – Availability of alternate recovery locations) for IT systems and staff.
- 9 – Determine recovery time and recovery point objectives.



Building A Plan For Your Business Security

## PRIME INVESTMENT SCHEMES WARNING

The Ontario Securities Commission and Law Enforcement Agencies are warning investors about legitimate sounding offers like “Prime Bank Notes”, “Prime Bank Debentures” and “Roll Over Programs” being used as a means to lure individuals into illegal scams. The word “Prime” is meant to refer, generically to reputable financial institutions. Persons promoting these schemes lead prospective investors to believe that they are being invited to participate in an otherwise secret trading regime. Investors are usually required to sign non-disclosure and non-circumvention agreements which prevent them from disclosing to any persons the identity of the parties involved in the investment programs and the terms of the transactions. Promises made to investors of above average returns or guarantees of unrealistic rates of return within a short period of time (20% return per month) are normal and little or no information is provided to investors about the trading programs. Legal looking documents which often use technical language are used in an attempt to confuse investors. References made to “High Cash Trading Programs” or “High Yield Investment Programs” are examples of these scams. Anyone solicited to invest in a “Prime Bank” investment scheme should be aware and remember *“If it sounds too good to be true, it probably is”*.



Safeguarding Your Money From Crooks

## IDENTITY THEFT

The danger of digital identity theft causes more worry for consumers than the war in Iraq. Identity Theft the fastest growing crime in North America, is second only to the World Trade Center attacks in terms of impact on consumer awareness of personal security issues, according to a study by Opinion Research Corporation. The study also found that, despite increasing awareness of Identity Theft, more than 40% of consumers have failed to implement even basic security protection.

Of those who had implemented security measures, 39% had installed antivirus software, 21% had changed where they stored personal information and 19% had reviewed the security policies of their internet service provider. Contrary to some views, Identity

*In 2001 86,000 people filed Identity Theft complaints.*

Theft is about numbers and money. A recent study by Meridian Research projects that by 2006 the financial institution sector alone will lose \$8 billion across North America. In addition, an estimated 500,000 to 700,000 people a year become victims of Identity Theft, while only 86,000 people filed Identity Theft complaints in 2001. Many of those people suffered significant financial loss. Furthermore when terrorists exploit Identity Theft, the financial and human costs as a whole can be catastrophic. Sources: Cnet and Vnunet.

## EMPLOYEE SCREENING – PAY NOW OR POSSIBLY PAY LATER

It pays to know exactly who you are recruiting, in our January 2003 newsletter we touched briefly on this issue, now lets take a closer look. Pre-employment screening goes beyond uncovering CV fraud, it also checks prospective employee’s history for theft, workplace violence and negligent performance of duties, substance abuse, ethics or work history. If employers fail to detect problem employees right from the start, they risk troubled times for the rest of their staff and the future of their businesses. Recently a major Toronto employer failed to conduct such a check on a new hire, within a few months the employee was found to be passing counterfeit money on the job. As there was a union in place, by the time the employee was let go with an exit package, the cost for lawyers, an internal investigation and staff disruption the final cost exceeded an estimated \$60,000. The cost for a background check probably less that \$ 150.00 and yes the employee did have a record for fraud, theft and passing counterfeit money.



Don't Be Taken For A Ride

LTD & Associates Inc.  
South Sheridan Executive Centre  
2910 South Sheridan Way  
Oakville, Ontario  
L6J 7J8

Phone: 905-829-8105  
Fax: 905-829-8326  
E-mail: info@ltdsecurity.com

*Investigative & Security Research Consultants*

[www.ltdsecurity.com](http://www.ltdsecurity.com)

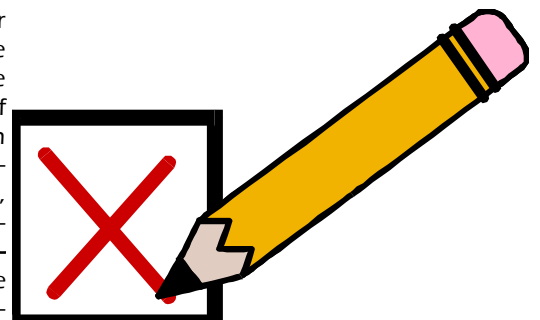
### Recent LTD Affiliations

*Ltd & Associates Inc. are proud to now be associated with the following professional organizations:*

- *Council Of Private Investigators Ontario.*
- *American Society For Industrial Safety International (ASIS).*
- *Investigators Of America.*
- *Asian Security Web.*

## INTELLECTUAL PROPERTY-PROTECT IT

What is it, quite simply the opposite of tangible property, it is anything you can't see, touch, smell or hear and therefore quantify. The mainstays of Intellectual Property (IP) are copyright, patent, trade-mark and trade secret law. As a business owner in order to protect your (IP) you must first evaluate it. For example how would you feel if you're competitors had your customer list, do you have a unique name for your products or services what if someone else started using that name, do you have materials that you wouldn't want someone else to use. There are commonsense ways to protect your (IP), don't leave important papers lying around, keep it off computers used by general office staff, build firewalls, divide information between those employees who need it and those who don't. **Copyright**-having your creative work protected gives you the right to the unique way you express your idea, but not the idea itself. You must register your copyright with the appropriate government agency, which can last for the life of the author plus 50 years. **Trade-Marks**-this is word, symbol or design that distinguish the good or services of one person or organization from others in the marketplace. A Trade-Mark can be registered for 15 years. **Patents**-are government grants that give inventors exclusive rights to their inventions. The patent protection applies in the county that issues the patent, in Canada this protection extends for 20 years. Eighteen months after filing the document is made public, so others can learn from your discovery. **Trade Secrets**-if you have a formula or process you want to protect but don't want to patent it because you don't want to share it with anyone, you have a Trade Secret. This is the world of (IP); ignore it at your peril. Source: BellZinc.



Business Solutions