ROYAL INDIAN RAJ
INTERNATIONAL CORPORATION®
• NEW YORK • VANCOUVER • BANGALORE

The Digital Assassination Of A Company

Losing a Billion: The Economics of Cybercrime

"How Royal Indian Raj International, its Investors and Clients Have Been Financially Compromised By Digital Criminals"

An Open Letter to All RIRIC's investors, customers and concerned individuals:

Management feels that this mater is of such fundamental importance to the company and it's investors and clients – and to all readers – that they have asked me to comment on both RIRIC's situation, and to the unfolding and universal problem of digital assassination in general.

If you are an investor or client you probably know RIRIC has faced two historic problems: The sudden and unexpected Bangalore Municipal Regional Development Authority/Government Land Freeze in India that has now been resolved to the satisfaction and benefit of the company. And in fact, to the satisfaction of the over 650 developers who's projects were also stymied because of the unforeseen government action.

And further, that the company and management (in many cases personally) have been subjected to an intensive and ongoing Internet digital assassination and smear campaign conducted by a disgruntled former communications/media employee, William (Bill) Zack and a SEO consultant Sharon Dobson.

You should note that a Federal Court Order ordered the web site shut down in 2008. He complied (outwardly), but moved it offshore and continued propagating his false allegations out of the courts jurisdiction.

They teamed up and as part of their ongoing malicious web assassination campaign they contacted David Bains, a Vancouver Sun columnist (no longer with the paper) who, looking for a sensational "scoop" and with apparently no knowledge of the Indian Realty market wrote a series of thirteen articles over a five-year period. Nine of which

were written in a nine-month period in 2008. All without the benefit of any interviews with company personnel. Sadly this "columnist" just used uncorroborated "third-party" misinformation and totally ignored the viable and well-documented business and legal material that the company had offered him for review, and began asserting that it was just a stock scam with the result it instigated the British Columbia Securities Commission (BCSC) to investigate. And thinking he knew more and was smarter than the BCSC investigators continued to do so even after, and despite the fact, that the regulator dismissed all allegations regarding this.

http://finance.yahoo.com/news/british-columbia-securities-commission-dismisses-201600605.html

In managements opinion this continuing disinformation campaign is a malevolent and premeditated criminal conspiracy using the unregulated Internet as a weapon to diminish RIRIC's ability to control resources and to damage the business and institutional credibility, and to sabotage any and all of the company's business, investor and customer relations and the company's financial wherewithal.

This was done utilizing RIRIC's stolen customer, shareholder and alliance partner lists thereby incensing customers and shareholders and alienating alliance partners by impugning RIRIC's good and valuable reputation. Malicious and fraudulent traffic was instigated and directed to internet "rumour" sites with specific instructions on what to do and say in coordinated attacks in order to panic customers and to influence regulators, law enforcement officials, the media and alliance partners both in North America and in India, all in an effort to egg-on vexatious investigations and actions.

All government reviews including the Untied States of America Securities and Exchange Commission have concluded that the company has done nothing illegal. But these campaigns have cost hundreds of millions of dollars in lost sales and immense 1st to market advantage. A short list of the lost financial opportunities resulting from these attacks are staggering:

- Suspension of Brands such as The Jack Nicklaus Design Exclusive India Wide Golf Brand
- Nicklaus Academies - India Wide
- Choice Hotels India wide 15000 Room initiative
- Phase 1 Lot sales of $400M
- The erosion of Royal Garden Villas Pre-Sales revenues of $40M which effectively prevented;

- The $300 M sell-out of Phase 1 in 2009 and the

domino effect of cancelling Phases 1B

- The cancellation of an Initial Public Offering (IPO) in 2010-2011
- Loss of Sales and Investor capital of $500M - $700M annually for 5 years
- Loss of between 1000 to 1500 sales inquires monthly estimated to be between 60,000 to 90,000 inquires over a five-year period
- Loss of financial arrangements
- The degradation and loss of Physical Infrastructure
- Lost opportunities in closing large land options in Bangalore, which were time-bound
- Loss of 1st to Market Position
- Loss of Reputation

As you can see these attacks not only affected the company's ability to proceed on its 1st to market initiatives but also affected our investors and buyers – thus it directly affected you!

(For further information regarding the continuing cyber assassination and media attacks against RIRIC please see the following press release -False Media.)

http://www.royalindian.info/1/post/2013/02/royalindianrajinternationalcorporationrespondstofalsemedia-cyberbullyingattack-orchestratedbydisgruntledformeremployee.html

However you will be pleased to learn that we are making substantial progress but not without considerable effort, as all this has had the effect of "working with one hand tied behind our backs."

All this being said the intent of this release is not so much to rehash these specific civil and criminal libels and the resulting financial costs to you and the company, but to create an awareness in how easy it is to assassinate both the reputation and the viability of a company or its personnel anywhere in the world – by one or a few angry and vengeful individuals!

This is not just about computer security any more – it's cyber crime plane and simple - from stealing financial and technical information, identity theft, digital piracy, transaction based fraud, denial of service or personalized digital assassination of

character and companies to name a few.

Most of you will probably be aware of the developing worldwide outrage regarding cyber bullying directed towards individuals, but there is another equally or even more damaging snake laying in the grass.

The old saying used to be that: “I saw it in the newspapers so it must be true, to the newer version - I saw it on Google so it must be true.”

Here is one example of how this can affect a company:

In 2008, a teenager on CNN’s iReport (its “citizen journalism page”) falsely reported that Steve Jobs had suffered a heart attack. The results? This teenager’s digital attack caused one of the worlds best known brands to lose hundreds of millions of dollars in stock value within minutes.

The average person just does not have the time or inclination to delve deeply into any given subject so that the typical person considers what they see on the Internet as being entirely true and factual and for the most part posted by honest people.

Excluding the Internet savvy – most of us are lagging far behind in realizing the enormous power of the Internet. This even includes many of the media who utilize the web as a resource.

Unfortunately, on the web no company or person is bullet proof. Those attacking you can, and in many cases do, hide behind stalking horses. Any one can post what ever they want on the web. Unlike the press of old, there is no one to verify the accuracy or veracity of *anything*. And digital assassination becomes even more effective – synergistically so - when other’s are knowingly enlisted, or as dupes and/or co-opted into achieving the instigators objectives.

In their book; Digital Assassination by Richard Torrenzano & Mark Davis. St. Martins Press, the authors write:

“If you want to intentionally defame someone, it’s an easy process…

The Internet has power that no other media has ever offered. Power in the form of instantaneity, 24/7 global reach, eternal memory, deep search capability, and instant retrieval.

For people, brands, or companies attacked on the Internet. Google’s algorithms assure that every defence will hype every attack – and every counter response – for as long as

the… of a fight is interesting to onlookers. (By the very act of Googling the subject).

…new technology… allow a vengeful individual to have an impact as never before."

Cyber assassination is a form of asymmetrical warfare with the attacker always having the upper hand/advantage by being able to strike/attack first."

So why don't people sue?

- It's very expensive
- It usually takes a court order to take down a site as Internet service providers jealously guard their fiefdoms
- Smart digital assassins hide their tracks
- By necessity, laws usually lag behind progress. This seems to be doubly true with regards to the Internet and content
- An example of the legal complexities involved, in the U.S. service providers are considered carriers (like telephone companies) and are not legally responsible for content. Content providers, however can be held responsible but as mentioned the clever ones are virtually impossible to track down using fake address's, using anonymizer's or an anonymous proxy that are untraceable on the Internet or by using offshore sites
- Or they hide themselves by using a preloaded credit card and bogus information and access the Internet using a wireless enabled coffee shop

The costs involved are astronomical. Not including the direct damage costs incurred as a direct result of cyberattacks. This is reflected in an article in Forbes:

"… the unfortunate truth is that every individual, company and government entity faces significant risk of becoming victims of cyber crime. And while the costs in time and money required to address holes in our cybersecurity stagger the imagination the question that law abiding people are asking now is, "how we can manage the risk," and punish the perpetrators."

Forbes Magazine – Dec 24, 2012 – Article The Economics of Cybersecurity by Thomas Stockwell. Pages 47-50

And Thomas M. Stockwell: Deloitte writes:

"Most telling is the increasing average time it takes for corporations to counter cyberattacks. In 2011, it was 18 days (average cost: $416,000). In 2012, the time rose to 24 days (average cost: $592,000), an increase of 42%, according to that 2012 study."(These costs are speculative.)

"Over the past few years it has become abundantly clear to me that for to long outdated laws and regulations designed for a previous era have allowed subversive elements to work outside the legal parameters of a just society. There is one small light however. India has taken a proactive step to come to grips with this endemic problem with the implementation of a new Information Technology Act as recently Gazetted:"

"The Gazette of India Amendment Act of 2008 – Published by Authority, New Delhi, Thursday, February 5, 2000

The Information Technology (Amendment) Act, 2008 (5th February 2009)

An Act further to amend the Information Technology Act, 2000

66A Any person who sends, by means of a computer resource or a communications device,

(a) any information that is grossly offensive or has menacing character; or
(b) any information which he knows to be false, but for the purposes of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or any electronic mail or electronic mail message for the purpose of causing any annoyance or inconvenience or to deceive or mislead the addressee or recipient about the original of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine"

"As you can see any company, brand, personal reputation, product or stock can now be digitally assassinated with immunity – in effect – murdered at the speed of light!

And in our case the personal vindictiveness and selfishness of the cyber attacks directed towards the company and management has also harmed so many people and impeded innocent investors and customers from realizing the creation of value over the years and financial gains."

As a victim that now knows first-hand the seriousness of this problem we are asking for the updating of the Canadian Criminal Code to recognize that in today's world you don't have to use a club to assault. And to recognize that there are modern forms of attacks that did not exist in the past. We need the Canadian Government to implement modern

cyber laws equipped with enforceable deterrents and tools – both criminal and civil – and to lobby other nations to do the same in order to stop these types of criminal assaults and make it so that there are no “off-shore” sanctuaries for these criminals.

As you can see that the way things stand now the Internet is analogous to the old Wild West. So upon reading this I would like you to consider that this is what has happened to RIRIC and also that it is entirely possible that sometime in your life, you or one of your loved ones could run afoul of the unregulated Internet.

Therefore I urge you to consider contacting your Member of Parliament and the Prime Minister that Internet assault and muggings, digital assassination and other forms of cyber-violence are assaults by another name only and that they are serious criminal acts that can have severe and sometimes catastrophic consequences and encouraging these measures be pursued.

I hope that the above has helped you in understanding this wide-ranging problem. As you can see digital assassination and cyber crime is a pernicious epidemic that has, and will, affect many innocent people.

Yours truly,

Manoj C. Benjamin
Chairman
Royal Indian Raj International Corporation

PS: Please think before you post and text.