

"Problems cannot be solved
at the same level of awareness
that created them".



H O F F M A N
& C O M P A N Y
Security – Risk – Business Continuity Planners



P: 705-726-1550
F: 705-726-0672
TF: 866-726-1550
www.hoffmanandcompany.ca

Business Continuity Planning

Given today's increased technology and necessity of network communications, Internet connectivity, expanding networks of electronic communication and specialized business processes, business continuity planning (BCP) for disasters are a rising priority on the agenda at executive boardroom meetings. For years you have been planning for the unlikely event of a disaster – for that single event that could bring your information infrastructure to its knees. But today, the unlikely suddenly seems more possible. Recent catastrophic events have heightened and yesterday's contingency plan is no longer adequate to keep today's information-centric organizations up and running. Hoffman & Company business continuity planning services are unique because we not only focus on your technology infrastructure, but also on the integration of your critical business functions and supporting information flows.

Hoffman and Company's Business Continuity Planning service is dedicated to helping you identify key business functions and processes by assessing your current level of preparedness and evaluating your contingency strategy so that it maps directly to your most critical business functions and information technology processes.

Business continuity planning is a process that identifies the most critical functions of your organization. A business continuity plan involves the long-range considerations for your organization's business survival after a disaster or catastrophic event. A professionally structured plan documents pre-arranged business response and recovery steps after a business interruption such as loss of telephone communications, loss of computer processing capability and loss of accessibility to vital critical facilities.

Recent events have proved that the resources of small and large corporations can be stretched to the limits in the period immediately following a disaster. According to statistics of those businesses that lost their records in a fire, 44% never re-opened their doors again, and 30% of those that did re-open failed to survive beyond three years after the fire¹. Why? Concurrently trying to operate a business, manage a disaster, prove losses to your insurance company and restore property proved to be impossible for three out of the four organizations. The statistics on floods are worse!

Business continuity planning can be a complex and expensive undertaking. Hoffman & Company understands this and provides value for your money by working to ensure that our clients gain the greatest possible benefit from the continuity planning process. Hoffman & Company Business continuity planning methodology is in accordance with the Disaster Recovery Institute's International professional practices. Our Certified Business Continuity Professionals (CBCP) are committed to the survivability and sustainability of your organization.

Avoid becoming a statistic. Seize the opportunity now to make the proper arrangements so that your business will not be counted among those that did not survive because they lacked the plan.

¹Association of Records Managers and Administrators

"In God we trust, everyone else we monitor"

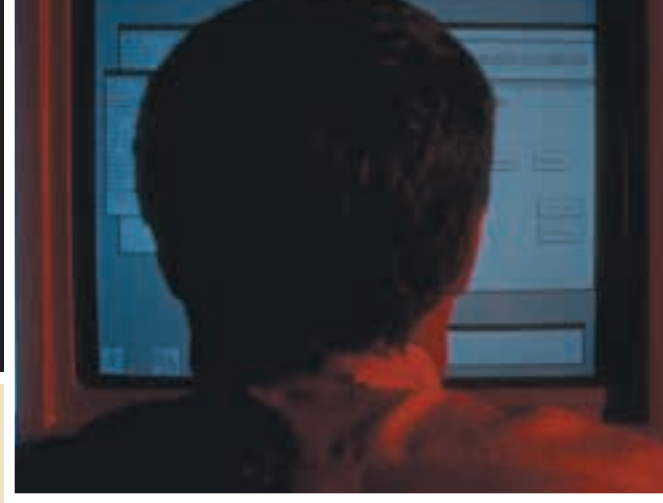
In the profession of risk mitigation and
in the protection of your organization's
assets, Hoffman & Company accepts the
responsibility for producing measurable
results in a manner that is ethical,
which in return contributes to the
forward thinking, survivability and
sustainability of your organization.

H O F F M A N
& C O M P A N Y

On Monday, September 10, 2001 we thought this great continent was secure...
on Tuesday, September 11, 2001 we learned different.

On Monday, September 10, 2001 people argued with their children over something so simple...
Tuesday, September 11, 2001 the same people could not get home fast enough to hug their children.

The terrorist attacks of September 11, 2001 have changed the political and emotional landscape of North America forever.



"Security is more art than science.
Few formulas will cover organizations' situations
and needs and that's the beauty and challenge
of security. Security is about Probabilities"



"If you can't measure it, you can't manage it".

Security is a serious matter.

Effective security management begins before an officer is hired or a camera is placed above a door.

Effective security management begins with a comprehensive and expertly informed plan.

The real business of protection of assets begins with a total knowledge of your organization's environment and assets combined with a comprehensive set of security policies, procedures and objectives. With that as an underlying principle, Hoffman & Company commit to providing service based on professional ethics and business practices with a systematic approach to investigation, analysis, response and reporting.

Hoffman & Company delivers the most current and complete technical expertise, flexibility and sensitivity toward our customer's social and environmental concerns, and a guarantee that all our efforts will be driven by the best interest of our customer.

Hoffman & Company demonstrate the commitment to service excellence by conforming to the requirements of ISO 9001, an internationally recognized quality management standard, which contains an inherent requirement for continual improvement. Operational and customer service records are maintained and regularly reviewed to verify objectives are achieved and customers are satisfied. The underlying principle and serious regard for security, risk and business continuity planning, and this corporate policy, are the driving force in delivering the high level of security risk and business continuity consulting services provided by Hoffman & Company.

Enclosed is our corporate brochure. Why not let us help you? No pressure. No nonsense.

Call us at 1-866-726-1550 to set up an immediate appointment. It is up to you. Act now, or just keep reacting. The time to manage risk is before it happens.

We hope to hear from you soon.

Kindest Regards,

A handwritten signature in black ink, appearing to read "T. Hoffman".

Terry M. Hoffman C.B.C.P., C.P.P.

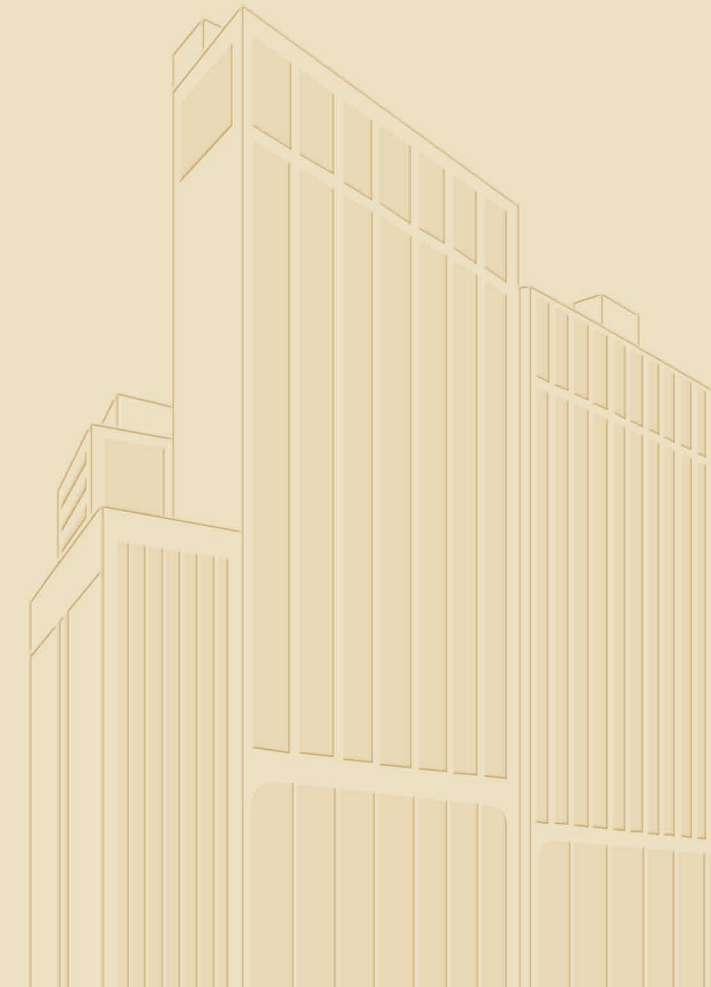
Security "Assets Protection Plans"

True security does not begin with just guards, technology or response training. The real business of protection of assets begins with a total knowledge of your organization's environment and assets combined with a comprehensive set of security policies, procedures and objectives. Employees and management need to be committed fully to a security plan and its program, as its awareness is critical to avoid "social engineering" forms of internal loss. Outside the human aspect of an assets protection plan is the provision of physical and electronic protection-in-depth barriers such as entry and search controls, intrusion detection, surveillance, alarm assessment and testing.

Collectively, engineered electronic and physical security systems, along with policy and procedure specific to each security layer, is intended to deter, delay, detect, assess and appropriately respond to an unauthorized activity. Examples of these activities include attempts to gain unauthorized access, remove or tamper with classified matter or steal/divert organizational assets. An example of a proactive deterrence and early detection approach would be to convert physical security access control systems to communicate directly with corporate networks.

An assets protection plan is customized to your specific organization. The plan, along with annual progress, proves that "reasonable efforts" are underway to protect your organization's assets. In turn, this could protect you against the legal liability of being found negligent in performing the duty of protecting your people, property and information.

The first-line approach to achievement is through a professionally formalized plan that encompasses both proactive deterrence and early detection.



Risk Management

Your organization should manage security risks by confirming the appropriateness of minimum security standards, supplementing these standards where necessary and eliminating unnecessary expenditures and administrative barriers.

Risk management for security is an itemized process which ensures that reasonable and cost effective steps are taken to protect the organization's personnel and prevent the theft and/or sabotage of corporate assets while ensuring the confidentiality and integrity of information stored, processed and transmitted.

Your company needs to formalize a plan that encompasses both proactive deterrence and early detection methods that protects your company against losses using a proactive security approach to help you qualify for insurance, reduce your premium and mitigate the risk that is excluded from your insurance coverage.

The Process Involves:

Assessing your organization's ASSETS (any person, facility, material, information or activity that has a positive value).

Assessing and identifying THREAT categories and intent, and motivation of all adversaries, estimating the frequency and degree of threat exposure relative to each critical asset.

Assessing building, location, people, equipment, operational and personnel practices and behavior to discover VULNERABILITIES.

Assessing the IMPACT of the Risks associated with threats and vulnerabilities.

Determining what administrative or physical COUNTERMEASURES may be implemented in order to reduce or eliminate one or more of the vulnerabilities.

Weighing the COSTS against the BENEFITS of each alternative countermeasure.

Making RECOMMENDATIONS AND DECISIONS.

Inadequate security and safety can create serious financial losses, cause liability, drain profits, damage morale and can result in loss of confidence by various business and social communities.