ASSOCIATION CONCEPTS
YOUR ASSOCIATION AND CONFERENCE MANAGEMENT EXPERTS!

Association Internal Risk Assessment/Disaster Recovery

DETAILED DISCUSSION

Please note – this document focuses on internal risks only; external risks are dealt with in another document.

Physical Security

Main Office – concerns: theft and destruction of property. Risks: break-ins; theft of property by the cleaning and maintenance staff; loss from fire. Theft by employees is a separate issue, with its own preventative measures.

Questions (building - security) – Is the building alarmed? What is the nature of the security (key, passcode, etc.)? Is there an active video camera system, and are tapes of activity kept? Where are the cameras located – lobby only; lobby and stairwells; lobby, stairwells and hallways? Is there an automatic locking/unlocking process for stairwell doors? Are extra precautions taken on weekends or evenings?

Questions (office - security) – Is the office alarmed? Can the alarm be cut or circumvented? If the alarm is cut, does this trigger an automatic response? How is access to the office controlled (key, passcode, etc.)? Do the police respond to intrusions?

Questions (cleaning staff) – Do cleaning and maintenance staff have access to the office outside normal business hours? If they use a passcode, is it one that is unique to them? Are they bonded? Do their employers provide insurance coverage in the event of theft of property traceable to their employees?

Questions (building – fire) – Is the office building fire alarmed? Are there smoke detectors or other fire-related sensors? Is the building sprinklered? Do any tenants store/use volatile chemicals? What steps are taken by them to prevent fires? How far is the building from the nearest fire station? Were fire retardant materials used in the construction of the building; if so, what are they?

Questions (office – fire) – Is the office fire alarmed? Are there smoke detectors or other fire-related sensors? Is the office sprinklered? Are volatile chemicals stored/used in the office? What steps are taken to prevent combustion of those chemicals? Is there a fire evacuation plan for the office? Are there fire extinguishers on-site, and have employees been trained in their use?

Off-site storage – most of the questions above also apply to off-site storage facilities, and the "cleaning staff/maintenance staff" questions can be extended to include staff at the storage facility.

Additional questions (off-site storage) – Are documents stored in a physically separate area? Is the area protected/separated by a wire-mesh cage, drywall walls, cinder-block walls or some other means? Is access to the storage area controlled? What measures are in place to control access (keys, passcode, etc.)? How is access to storage records granted? Is access supervised?

Data Security

Questions (desktop computer security) – Is there an appropriate regime for passwords on all computers (i.e. a mix of numbers, letters, other characters; minimum length; password change)? In the event of employee termination, is her/his password changed/removed by an administrator to prevent unauthorized access?

Questions (data back-up) – Is there a data back-up schedule for all computers/systems/networked drives/mail servers? Does it comprise both daily incremental back-ups and a weekly full back-up? Are back-ups checked for accuracy and readability to ensure media has not degraded? Is off-site storage used for back-ups? If so, how are they secured against theft, damage and loss?

Questions (back-up power supplies) – Are servers protected against power outages by back-up power supplies? Does the software supplied with the power supplies allow for a graceful automatic shutdown in the event the outage lasts longer than power is supplied for? Do the power supplies also provide protection against power surges, power spikes and RF interference? Are the power supplies checked periodically to ensure the batteries are charged and the supplies are fully operative?

Questions (virus and malware) – Do all systems (particularly Windows-based systems) have anti-virus and anti-malware software installed? Can virus and malware databases be updated automatically? Can system scans be run automatically? Does anti-virus and anti-malware software check incoming and outgoing e-mails and files being opened? If employees are able to download and install programs, browser add-ons and other files, are these files scanned before (or as) they are opened/executed?

Questions (remote access) – Do employees have remote access to the servers? On what basis is such access granted and how is it controlled? Is the access secure? Can log-in names and passwords be read over unsecured networks (such as those normally found in hotels, airports, etc.)?

Privacy

Questions (privacy policy) – Does the association have a published privacy policy, in accordance with PIPEDA? Has this policy been communicated to all employees? Has the association ever had a complaint lodged with the Privacy Commissioner? Did it result in legal action against the association? Does the association have a privacy officer? Where the association has chapters/branches, is each chapter/branch compliant?

Questions (records retention) – Does the association have a records retention policy (covering its dealings with members and its own information)? What types of records are covered in the policy? For how long are different types of records kept?

Does the association adhere to the policy? How does it prevent retention of records beyond the disposal date?

Questions (record disposal) – Does the association have a records disposal? Does the association have a policy covering the destruction of electronic records (logs, hard and soft copies)? Does the association adhere to the policy? How does it prevent retention of records beyond the disposal date?

Questions asked under Physical Security and Data Security are also relevant here.

Legal

Questions (employment agreements) – Do employees have employment agreements? Are these in writing? Do they define essential terms of employment (if any) and set out the disciplinary action to be taken in the event of breach of such terms? If there is a template for such agreements, has the template been reviewed by a lawyer and been found to be enforceable?

Questions (copyright) – Does the association have policies in place governing copyright arising out of materials developed by employees for the association? Are employees aware of this? Do such agreements extend to suppliers? Are suppliers who develop copyrighted materials for one client prohibited from using it for another?

Questions (signing officers) – Does the association authorize specific individuals, by by-law or by resolution, to act as signing officers for leases, contracts, investments, cheques, etc? Does the association have a policy to prevent a signing officer from having an interest in the instrument being signed (e.g., can an officer sign a cheque made out to him/herself? Can a signing officer sign a lease in which s/he is an owner of the leasing company or leased equipment?)?

Questions (Board of Directors) – Does the association have a code of ethics or behaviour, and a charter for its Board? Does the association have a policy and process regarding orientation of new Directors? Are Directors' term limits consistent with governing legislation/regulations (e.g., 4 years for federally incorporated associations; 3 years for Ontario (under proposed new legislation))? Does the association have methods in place regarding hiring of new employees/contractors to ensure involvement of more than one person? Is the Board aware of legislation governing employees and/or contractors? Is the Board generally aware of legislation relating to non-profits? Does it communicate this to chapters/branches as appropriate? Are by-laws in conformance with legislation/regulations? Do they keep pace with changes?

Insurance

Questions (insurance) – Does the association maintain any of the following types of insurance: Directors and Officers, public liability, "errors & omissions" type insurance (against fraud, theft, or other acts by the partners, managers or employees), business continuity insurance, and insurance on leased vehicles? What are the terms of such insurance? Are the types of insurances in place reviewed regularly to ensure the association has appropriate coverage?

Questions (events) – Are events covered under the public liability and/or Directors & Officers policies? If the association is presenting an event at which alcohol is available, does it have an insurance rider on its public liability policy? Will "serve smart" or similar staff be used to serve the alcohol?

Finance

Questions (finance) – Over the most recent five years, has the association made or lost money? If the association has lost money, how significant has the impact been on members' equity/net assets? What is the trend for revenues – growth, shrinkage or little/no change? Does the association reserve a portion of revenues or surpluses against contingencies? What percentage? Currently, how many months' expenses would this reserve cover (assuming no revenue)? Does the association have a reserve for new products/services, or for other major initiatives? Do the Directors have a sufficient understanding of finance to allow them to participate meaningfully in budgeting, review of monthly statements, year-end financial review, and financial controls discussions? Do the Directors actually participate in these discussions? Does the association have its books audited/reviewed? When was the last time a new auditor was appointed? What is the relationship between auditor and staff? What is the relationship between auditor and Directors (including the officers)? Has the association ever had a qualified or adverse audit opinion? What is the involvement of the Treasurer in preparing the draft budget? What is the involvement of the Board members in reviewing the draft budget and finalizing the budget? What financial controls are in place? How are these controls monitored? Does the association have anti-money laundering and anti-fraud processes in place (e.g., mandated 2 signatures for each cheque or other financial instrument; naming signing officers by by-law or resolution; prohibiting an officer from signing anything in which s/he may have an interest (including cheques made out to themselves))?