Risk Management Considerations for Creating a Culture of Security in Your Workplace

People work best when they feel emotionally safe and secure. They focus their energy on solving problems and doing their best. Secure employees are also happier and more satisfied employees. How do you promote a culture of security? Here are a few ideas to get you going:

Get the Ball Rolling

- Set the tone and lead by example. Executives must show their support for security policies and procedures.
- An organization committed to ethics and compliance can reduce exposures to risk such as bribery and fraud.
- Include employees in the creation of the policies. Employees are an excellent resource and will make valid contributions. Furthermore, if they are involved in policy creation, they will understand the reasoning and will take ownership.
- Establish an employee participation program that encourages employees to report security breaches.
- Protect "whistleblowers". Organizations need to encourage employees to come forward with information to ensure a safe workplace because awareness of an incident is the only way to correct it. Reporting systems, when used properly, help bring managerial attention to issues early on. Early detection of misconduct can assist in reducing financial losses, protecting employees and maintaining a positive corporate reputation.
- All visitors, contractors and suppliers should be required to report to reception upon arrival.
- All guests should sign in and note their company name, their name, who they are visiting, time in and time out. These records should be logged.
- All visitors should be given an ID or visitors badge.
- Visitors should never be left alone.
- Do not tolerate solicitors. Ask them to make an appointment with the appropriate person if they're really interested in earning your business. Some solicitors are only there to scope out the business.
- Consider installing security cameras.
- Employees should feel free to politely challenge visitors without a badge. Ask them who they're visiting. If they can't state a name, take them to reception.
- Valuables should be hidden and locked. This applies to articles left in vehicles as well as desks and public spaces.
- Use key control. Create a procedure for those responsible for opening or closing the office. This includes checking washrooms, closets, or anywhere someone might be able to hide. Hard keys should be numbered and assigned to specific individuals.

Password Protection

- Employees should immediately change default or factory setting passwords on their computer.
- Passwords can't be based on personal or corporate information.
- Secure passwords should have upper and lower case letters in addition to numbers and special characters. They should also be a minimum of 8 characters long.
- Employees must safeguard their passwords and never share them with coworkers.
- Passwords should be changed every 30 days and the same password shouldn't be used within a 24 month period.
- Computers should be set in a locked mode when not in use.
- Out of office messages should be vague as to when you are returning.
- Automatic "remembering" of passwords should be disabled.
- Do not write your password down or affix them to your monitor.

Online Protection

- Social engineering exploits human vulnerabilities such as our need to help or offer a quick solution in the interest of providing superb customer service.
- Social engineering involves an outsider tricking an employee into unknowingly giving away confidential information.
- Employees need to be trained in recognizing social engineering attacks. Some tactics may include:
- A caller refusing to give their contact information (i.e. who they are, who they represent)
- A caller rushes through their request
- Name dropping throughout the conversation
- Resorting to intimidation when questioned
- Asking “odd” questions.
- Stating a senior member in the organization needs the requested information immediately.
- Requesting confidential information.
- Requesting changes to confidential information like bank account numbers.

Additional Suggestions on Creating a Culture of Security

- Define how information is to be destroyed – what must be shredded vs. what can be thrown away or recycled.
- Dumpsters should be located in a secure area that isn’t easily accessible to the public.
- Employee names and personal information should never be given out.
- Suspicious phone calls, visitors and packages should be reported to the police.
- Note that it isn’t appropriate for employees to distribute client information.
- All packages and deliveries should be received by reception or shipping. Any unclaimed packages should be checked out immediately.

Communicating Policies and Procedures

- Policies and procedures should be written using simple, easy to understand language. Avoid using jargon and acronyms.
- Post security policies on your intranet or a bulletin board.
- Encourage managers to explain and talk about the policy with employees.
- All employees should sign an acknowledgement form stating that they have read corporate policies.
- Audit policies and make updates as needed.

The times have changed and it is important to guard against physical and electronic security threats. Make sure your organization recognizes where breaches in security can occur. Let employees know that they are important in your organization’s defence against intruders and social engineers. Education and training are the key to protection.

While Intact Public Entities Inc. does its best to provide useful general information and guidance on matters of interest to its clients, statutes, regulations and the common law continually change and evolve, vary from jurisdiction to jurisdiction, and are subject to differing interpretations and opinions. The information provided by Intact Public Entities Inc. is not intended to replace legal or other professional advice or services. The information provided by Intact Public Entities Inc. herein is provided “as is” and without any warranty, either express or implied, as to its fitness, quality, accuracy, applicability or timeliness. Before taking any action, consult an appropriate professional and satisfy yourself about the fitness, accuracy, applicability or timeliness of any information or opinions contained herein. Intact Public Entities Inc. assumes no liability whatsoever for any errors or omissions associated with the information provided herein and furthermore assumes no liability for any decision or action taken in reliance on the information contained in these materials or for any damages, losses, costs or expenses in a way connected to it. Intact Public Entities Inc. is operated by a wholly owned subsidiary of Intact Financial Corporation. Intact Design® and Risk Management Centre of Excellence® are registered trademark of Intact Financial Corporation or its affiliates. All other trademarks are properties of their respective owners.

intact public entities