12 EFFECTIVE SECURITY HABITS

1 **Run the Latest Version of your Organization’s Software**
Software vendors are constantly updating software to patch vulnerabilities

2 **Eliminate Unutilized Software that your Organization Does Not Need**
An unneeded application is an unneeded risk

3 **Know where your Sensitive Data is Stored**
Assess the value of your organization’s assets and understand what you need to protect

4 **Focus on the Right Threats**
Identify your organization’s top threats and eliminate by level of risk

5 **Practice Risk-Based Patching**
Patch quickly but by system value, vulnerability score and threat level

6 **Educate Users on Social Engineering**
Phishing is by far the most used and successful attack method

7 **Keep your Configurations Consistent**
Do the same thing, the same way, every time. Make sure any change, once tested, is consistent across all systems

8 **Use Least Privelege Access Control**
Give the minimum permissions to those who need them to do an essential task

9 **Minimize the Use of Administrative Privileges**
Minimize Super-Admin privileges on accounts as possible. Credentials are far less likely to be stolen and admins are easier to track if there are fewer of them

10 **Adopt Role-Based Access Control**
Apply least privelege to computers and configurations according to the tasks that need to be preformed

11 **Establish Smart Monitoring Practices & Timely Response**
Monitor anomalies and respond to them

12 **Seek Help From A Trusted and Reputable Security Vendor**
Recognize your weaknesses and reach out to the appropriate security provider

Address: Meteor Office Park, Sokolovská
100/94, 186 00 Praha 8, Czech Republic
Address: 1550 Metcalfe Street, Suite 502
Montréal, Québec, Canada H3A 1X6
Tel: 1.888.982.0678 Fax: 1.514.982.0362