WHITELISTING/BLACKLISTING

What is a whitelist and blacklist and how does it apply to a small business?

Whitelisting and blacklisting are two methodologies to control access to websites, email, software and IP addresses on networks. Whitelisting denies access to all resources and only the "owner" can allow access. Blacklisting allows access to all with the provision that only certain items are denied.

Whitelisting has advantages in that you control access to the website or virtual resource you want your business to use, however, is less dynamic and more restrictive in terms of ease of use and versatility. This is a control mechanism where you deny access to all resources by default then allow access to resources by name. Think of your home, where only you and your family can get access the front door. Everyone in your family would have a front door key, but some individuals don't have keys to every door. You may have a shed out back that only you have they key because dangerous chemicals are stored there. The disadvantage is that not everyone in your family has open access to the shed and would have to ask permission to get something out. Now, that may work for a small family, but would be unworkable unless the number of employees requiring access is small. This type of access control is useful for financial or personnel records, where a business might have only 2-5 employees who access these files, software or websites.

Blacklisting is advantageous in that it allows free and open access to any email, website, IP address or software as long as it's not a security risk. This is the concept that all web traffic is allowed, and certain items are disallowed by name or circumstance (aka security risk). For instance, say you were at a supermarket, and you want to have access to the store, all the products, and every aisle. A backlist is a list of restrictions based on a circumstance, say the person is a known shoplifter or under age. It doesn't restrict access to everyone, but restricts certain shoppers based upon a known risk or circumstance. The disadvantage is enforcement – as a business you have to enforce access each time someone enters the store or tries to purchase an item. As a small business owner, this type of access control might be useful to restrict access to websites that might interfere with job performance, such as gaming sites, unless of course you are a gamer!

What are some specific examples of white listing and blacklisting that may apply to my small business?

Software
- Whitelisting
  - Employers restrict access to applications used by a select number of employees to perform their role for the business – such as accounting, human resources, and/or payroll. Access would be restricted on the machine or server used for these functions.
- Blacklisting
  - Employers restrict access to games or prevent applications, which could contain malware.

Email
- Whitelisting
  - Employers would only receive emails from clients, or other employees.
- Blacklisting
  - Employers would block domains who are known to send spam, junk, or phishing emails.

Websites
- Whitelisting
  - Employers restrict access to websites used by a select number of employees to perform their role for the business – such as accounting.
- Blacklisting
  - Employers restrict access to sites which may interfere with workplace performance such as: pornography, gaming sites, social networking.