A “Logic Bomb” isn’t really logical, it’s a virus, designed to take down your corporate network and disable existing systems that may monitor data, protect it, back it up or access it. A logic bomb is designed to multiply like any virus and spread throughout a network multiplying its effects.

In a Wall Street Journal story an example provided, depicts an employee at Fannie Mae, knowing he is about to be fired commits an act of workplace violence by installing a logic bomb set to detonate almost 3 months after his departure. The detonation would have taken the organization off line for almost a week and cost millions and millions of dollars.

In this true insider threat story, an observant programmer, still employed noticed the code and disabled it before the damage could be done.

Think for a moment about your small business and how you would get in if you lost your keys. Maybe through an unlocked window? And if a burglar knew what you knew about where you hide that extra key? How much damage could he do, knowing what you know? Insider threats pose the same problem. They know the ins and outs of all systems in place and can wreak havoc on your operation while they are employed and sometimes after they are let go.

The problems begin when we put people in a trusted place. They are granted access because that’s their job to perform certain duties and they are granted carte blanche access. Ultimately IT security is a people problem and needs to be addressed that way.

Preventing Insider Threat

1. Limited Sources; only grant access to a few trusted sources. Minimize the amount of staff that has access to whatever systems in place.

2. Due Diligence; in the information age, our lives are an open book. Background checks from information brokers are very necessary. Not doing a background check increases your liability.

A person previously convicted of a crime just might do it again.

3. Limit Access; even a good apple eventually can go bad. By restricting the access to even those who are in a trusted position, in the event they turn sour, they can only do limited damage.

4. Defense in Depth; audit, audit, audit. This is all about checks and balances. Separation of powers. Multiple layers of authorization. We've all watched the movie where in order to launch the missile there were 2 keys held by 2 people, who pressed 2 buttons in order for the missile to launch. Put systems in place that facilitate someone always watching over someone's shoulder. This way the bad apple can't hide or execute their malicious intent.

5. Prosecute the Guilty; in the event of a breach of trust, make an example of the person that others won't forget. Public hangings set a strong deterrent.

Robert Siciliano personal and small business security specialist to ADT Small Business Security.