



# 2-Minute Offense



*Analysis of Current Digital Threats & Countermeasures*

## EXECUTIVE SUMMARY

This week's FLAILCON remains at 2. Ensure that you have updated all of your Microsoft systems from last week's *Black Tuesday* update. There have also been significant spikes in SPAM floods affecting network bandwidth over the past week. Examine your filters for ingress traffic to ensure they block unwanted traffic and examine your outbound traffic to ensure that your organization is not an unwitting SPAM purveyor.

This week we focus on a reality that very few business owners understand: security is about more than technology. It is a process - a dynamic and continual process. Oftentimes, it's not the business owners' fault for thinking this way. They are not security experts and therefore rely upon security vendors for guidance. But security product vendors are focused on one thing: selling more product.

Business owners need an objective partner who is interested in the welfare of their entire security program, not just their security products. If technology worked, we would all already be safe. Below, Maverick outlines some of the reasons why technology alone is not enough, and that - as security pundit Bruce Schneier has said - security is a *process*, not a product.

## DEFENSE FOCUS

VOLUME 3 NUMBER 02

*"Security is a process, not a product."*

These words spoken by Bruce Schneier have never been more true. Regardless of how far security technology has advanced, it is not ready to replace the human. It is a component of an overall security process, not the process itself. Vendors of security products like anti-virus, anti-spyware, and firewalls, while providing a useful service, are interested in selling more products. It is the reality of their business model, and the reason why companies like Symantec have bought up complimentary services like intelligence and have given them away as part of security packages. Their focus is on the sale of products, not the complete security solution.

Let's examine the issue a little deeper. Anti-virus provided by the biggest 3 vendors, Symantec, McAfee, and Trend Micro, is signature-based. This means that the product relies on fingerprint-like signatures that malicious code leaves after it executes. Signature file anti-virus has been around since the early 1990s. This defense was effective in the mid-90s because at the time viruses were passed between computers by floppy disks, not the Internet. But with the advent of the Melissa virus in 1999, signature file AV became obsolete. In a world that is instantly-connected, being able to stop only what malicious code you know exists is no longer enough. This is the primary reason why malicious code is still effective. Yet even more importantly, no quality of signature file AV can prevent a user from clicking on an email attachment. Only security awareness training, as part of your security process, can stop user mistakes.

There is a similar problem with botnets. Botnets are clusters of compromised computers used together to attack a larger target with overwhelming strength. There is no technology in existence currently that can prevent the creation of botnets because the problem is not about security technology but security process. Most often the systems that make up the botnets are home or small business systems compromised because of user mistakes. Social Engineering, the act of duping the user into making a mistake, is the problem. Again, security awareness training as part of your process, and not the use of better or newer technology, is the solution.

Last, look at security policy. There are technologies out there to help you perform policy audits, examining your systems to ensure that they meet the requirements of the policies. But no technology can write those policies for you, or know which policies are the best for your type of business. It also cannot change those policies over time to meet emerging threats and the changes of a dynamic security environment. Only a solid security process, using security experts crafting policies specific to your needs, can do that for you.

Technology plays an important and relevant role in a security process, but it is only one component. It is a tool that is wielded by security practitioners executing a complete security process. No amount of salesmanship can change that.

## WALL OF SHAME

### University of Idaho

Up to 70,000 SSNs, names, and addresses exposed on a stolen (unencrypted) laptop.

### MoneyGram

79,000 consumers' data is unlawfully accessed from a compromised server.

### NC Dept. of Revenue

30,000 taxpayers' files on a stolen laptop. Encryption level unknown.

## DON'T FORGET THE DUMPSTER, COPIER, AND PRINTER

When building up your list of things to consider, check, and secure in your environment, do not forget 3 critical things: your trash & recycling, your copier, and your printer. Organizations must consider what they are throwing out, whether or not it is company sensitive, intellectual property, or should otherwise be shredded. You must have a program in place to shred sensitive materials, and each of your people must be taught, when in doubt - shred it. Your recycling program can make you vulnerable too. Doing the right thing with recycling can put you at risk unnecessarily. Your policy should include this to prevent data loss through recycling.

Your copier and your printer may be one device, and may even be networked. In that case, it's called an MFP - Multi-Function Peripheral. MFPs pose three risks to your company. First, MFPs often come with hard drives or flash memory to hold the large graphic files prior to print. If they are networked, they can be hacked. Second, when you dispose of these MFPs, if you do not remove or at least wipe the hard drives within them then the data they possess on your organization is exposed. Third, carelessness with sensitive items left in the print tray of your MFP can expose your company too. Most organizations either use an outside cleaning service or have one provided as part of their building lease. These personnel are not yours and are not within your control. Sensitive materials should be removed from MFPs every evening when the facility is closed.