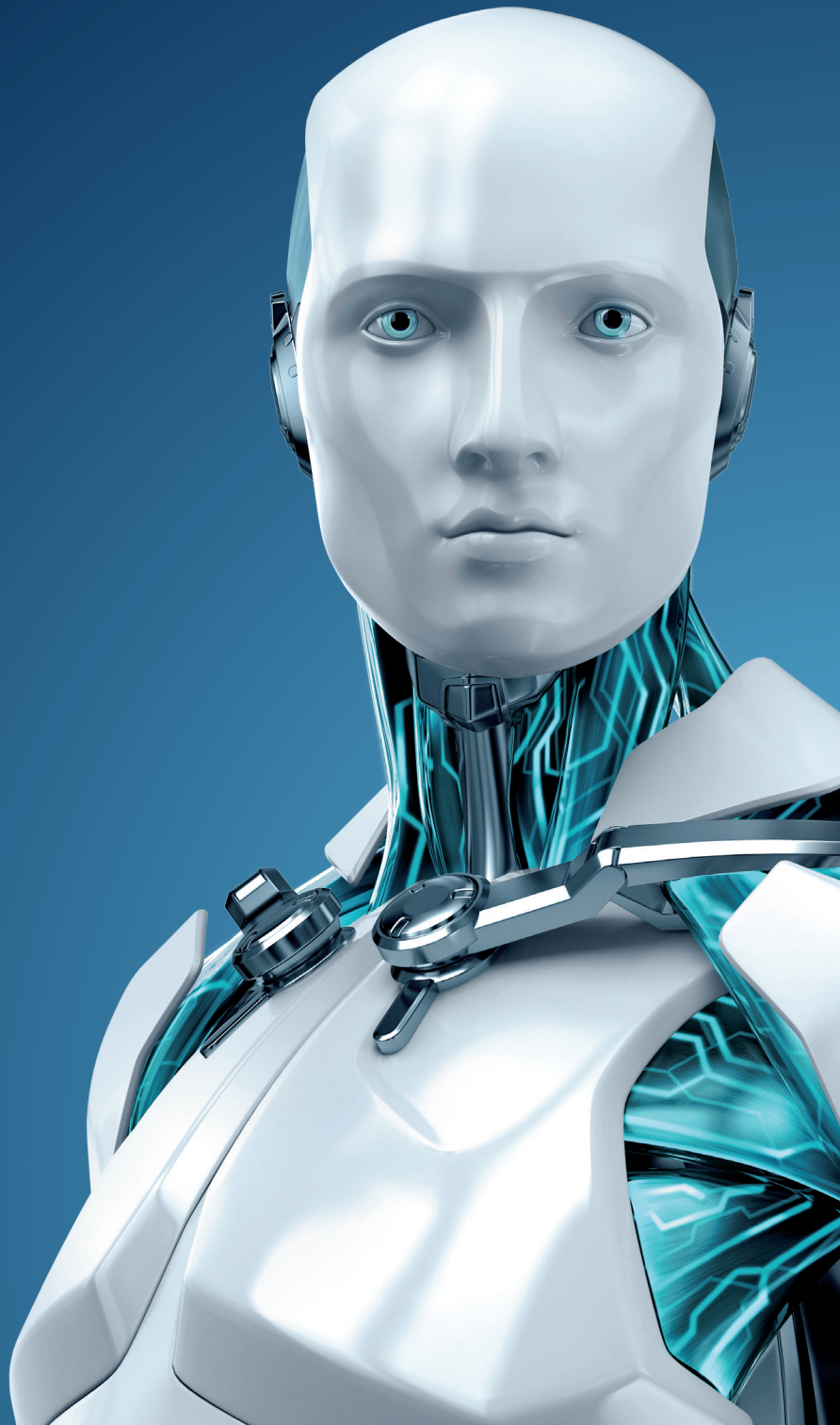
TECH BRIEF

Why your small business needs an information security policy and a WISP



ENJOY SAFER TECHNOLOGY™

WHY YOUR SMALL BUSINESS NEEDS AN INFORMATION SECURITY POLICY AND A WISP

By Stephen Cobb, ESET Security Researcher

A recent question about need cases for singular versus multiple policies got me thinking about how information security people talk about policy—and I realized it can be confusing. So here are some explanations about security, policies and a thing called WISP.

First of all, what does it mean for an organization to have an information security policy, singular? It means that the organization has stated and recorded its commitment to protecting the information that it handles. For example, here is what Acme Bicycle Company might say:

> It is the policy of ABC that information, as defined hereinafter, in all its forms—written, spoken, recorded electronically, or printed—will be protected from accidental or intentional unauthorized modification, destruction, or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

This statement of overall policy usually appears as the preamble to a series of more specific policies. For example, there may be a section on risk management:

> A thorough analysis of all ABC information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information.

There should probably be a virus protection policy. It that might say something like this:

> Virus checking systems approved by the information security officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures that all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

So there are multiple specific policies below the overall information security policy. There is another term you may see in this context: written information security program or WISP (not to be confused with Wireless Internet Service Provider).

WISP is a term that encompasses all relevant policies plus your organization's program for implementing them. I like the term because it implies something more practical that just a collection of policies sitting in a binder (although the WISP will likely sit in a binder too). Regular readers may recall that WISP plays a prominent role in some information security legislation, notably the law in Massachusetts, which says:

> Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards...

I won't go into the details about Massachusetts law, since the main points were covered in the earlier article[1], but suffice it to say I think that every business, large or small, needs to have a WISP. This may simply be an attachment to existing policies that says:

> **The ABC Written Information Security Program consists of the enclosed policies and the steps we take to enforce them, including dissemination of polices to all new employees and the regular training of all employees on how to uphold the policies in their work, together with a periodic management review of the program to ensure that all aspects of information security in our organization are appropriately addressed at all times.**

If you meet resistance when it comes to the not-inconsiderable effort of creating and executing a WISP, try persuading skeptics with a litany of examples of small firms that actually went out of business or suffered severe loss because of cyber criminals, many of whom could have been defeated if the victim had been on top of the problem. Where to find the facts? The highly reliable Brian Krebs has a sobering collection of small biz cases, constantly updated.

Why a WISP may deal you a winning hand

Suppose you run Acme Bicycle Company and have developed a new style of bicycle pedal. Will Joe Consumer, who just wandered into your retail store, ask to see your WISP before he buys pedals from you? Probably not. But suppose you're bidding to supply a lot of pedals wholesale to the MegaSports chain. Will MegaSports want to see your WISP? Probably.

I have seen the lengthy compliance documents that some large companies present to smaller companies with which they want to do business. Without a WISP, it is going to be hard to comply in a timely fashion, which means you could lose the business to a competitor with a security program already in place and documented. Here is language from one such document, which was attached to a juicy contract as a condition of doing business:

> **Vendor must have a written policy that addresses information security, states management commitment to security, and defines the approach to managing information security.**

And here are some questions another big vendor put to an SMB, again as part of the contract process:

- Are there documented policies and procedures for managing security?
- Does the vendor perform internal reviews of security policy and technical compliance?
- Are security policies and procedures disseminated to all vendor employees?

So getting your information security policy in order is not a wish list item or a "nice to have but not essential" extra for your business. Not only is a WISP essential to succeed in fending off the bad guys (who are most definitely targeting small businesses these days), it also helps you to win business.

1 Will of the WISP: Your company's Written Information Security Program By Stephen Cobb. http://www.welivesecurity.com/2012/04/11/wisp-your-companys-written-information-security-program/

Policy links that may help

Here are some links to free information and policy samples that can help you tackle the task of WISP creation and implementation:

- **Massachusetts Written Information Security Plan** developed by Buchanan & Associates of Boston. http://www.buchananassociates.com/Buchanan-Associates-Sample-Template-Written-Information-Security-Plan-WISP.pdf
- Common **misconceptions about the Mass Privacy Law.** http://charlandtech.wordpress.com/2010/01/25/5-common-misconceptions-about-mass-privacy-law-201-cmr-17-00-part-45-im-ok/
- **A Small Business Guide: Formulating a Comprehensive Written Information Security Program.** http://www.mass.gov/ocabr/docs/idtheft/sec-plan-smallbiz-guide.pdf
- A Sample Information Security Policy from **Advanced System Integrators.** http://www.asiopen.com/downloads/201CMR1700_WISP.pdf

If you're in the business of education, you can easily find other schools' security policies by using Google. For example, **The George Washington University Information Security Policy** can be found at http://my.gwu.edu/files/policies/InformationSecurityPolicyFINAL.pdf. Note that policies are one area where some "plagiarism" may be permissible. In other words, your organization may take policies from others and customize them to your needs. (Policies are a bit like recipes as far as copyright is concerned, but I'm not a lawyer, so you may want to check this, and you certainly shouldn't be reselling policies you didn't write.)

If you're in the business of government, then the security policies of other agencies should be readily available to you. There is an index of links to state information security policies at http://msisac.cisecurity.org/resources/state-cyber-policies.cfm.

Commercial vendors offer tools for implementing policy— for example, **Info-Tech's Security Policy Implementation**[2] tool.

2 Info-Tech's Security Policy Implementation. http://www.infotech.com/research/security-policy-implementation-tool