TECH BRIEF

Small Business Cybersecurity Survival Guide

ENJOY SAFER TECHNOLOGY®

SMALL BUSINESS CYBERSECURITY SURVIVAL GUIDE

By Stephen Cobb, ESET Senior Security Researcher

Computers and the Internet bring many benefits to small businesses, but this technology is not without risks. Some risks, like physical theft and natural disasters, can be reduced or controlled through sensible behavior and commonsense precautions. Harder to handle are the cybercrime risks like those posed by criminals who steal information to sell on the black market.

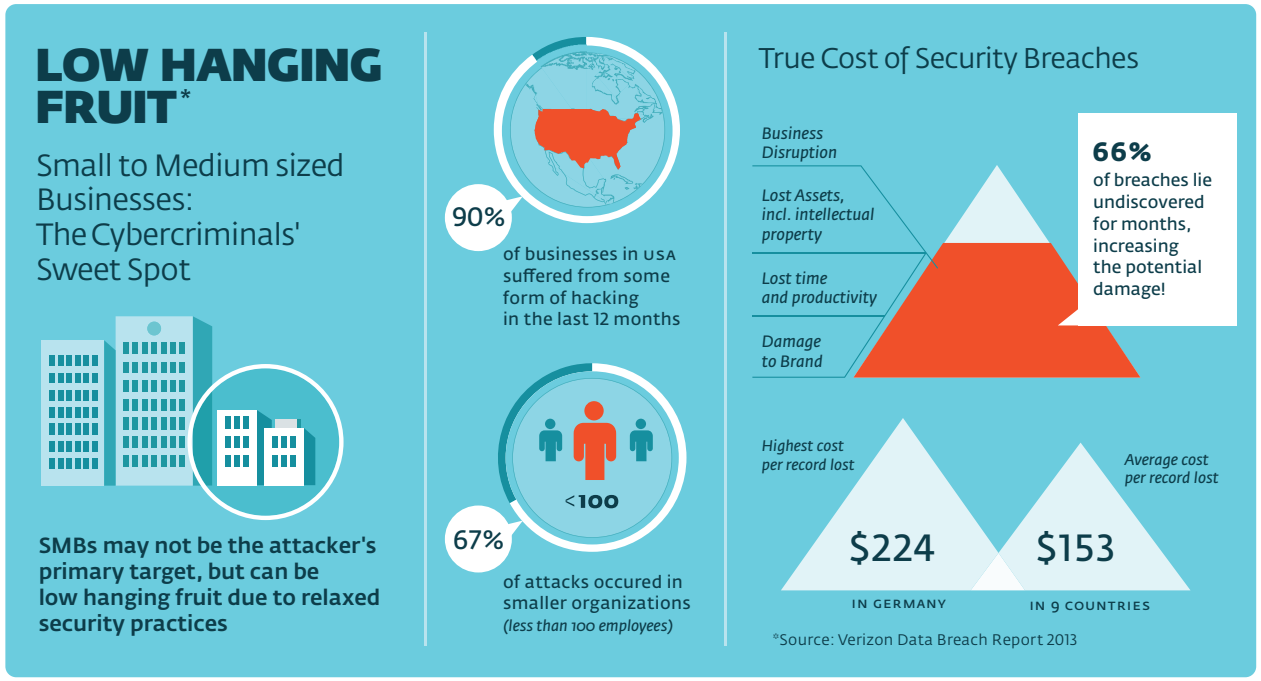
This cybersecurity survival guide will help you defend your business against cybercrime threats.

Personal information, that is, information that can be used to commit identity theft, is a common target of criminals. Even the smallest businesses are likely to handle some personal customer or vendor data worth stealing. Another popular target of cyber criminals is account information—from credit card data to bank account numbers, online banking passwords, email accounts, and user credentials for services such as eBay, PayPal, and TurboTax. All of these can be sold on the black market to other criminals who specialize in using the information in a wide range of fraud schemes and scams.

Consequences of Data Theft

Because most small businesses have account information and personal data that criminals could abuse, you need to remember that your business may be held responsible for the consequences of data theft—for example, if information about your customers is stolen and used for fraud. Some data is protected by laws and regulations, like HIPAA and PCI (for medical and credit card data, respectively). Many states also require businesses to report security breaches that expose personal data to potential abuse, whether it's a lost laptop containing customer details, or a thumb drive with medical records.

All of this means that, even though your company may be small, you must take a systematic approach to securing any data that is entrusted to you. As you go about the task of protecting your company's digital assets, you should



document your approach. This will help you educate employees about their security responsibilities. Furthermore, it is not uncommon for larger companies to require vendors and contractors to provide proof that they have educated their employees about security, and that they have put appropriate security measures in place. If a security breach does occur, a documented security program helps you prove that you were diligent in your efforts to protect information.

Steps to take

We've laid out a systematic approach to cybersecurity for you that goes from A to F.

- **A**ssess your assets, risks, resources
- **B**uild your policy
- **C**hoose your controls
- **D**eploy controls
- **E**ducate employees, execs, vendors
- **F**urther assess, audit, test

Let's look at each step in turn:

Assess your assets, risks, resources. List all of the computer systems and services that you use. After all, if you don't know what you have, you can't protect it. Be sure to include mobile devices like smartphones and tablets that you and/or your employees may use to access company or customer information. And don't forget online services, such as SalesForce, online banking websites, and cloud services such as iCloud or Google Docs.

Now go through that list and consider the risks related to each item. Who or what is the threat? Another good question to ask is: What could possibly go wrong? Some risks are more likely than others, but list them all and then rank them according to how much damage they could cause and the chances they might occur.

You might seek outside help with this process, which is why you need another list: the resources you can tap for cybersecurity issues. This could be someone on staff who is knowledgeable and security-savvy, or a partner or vendor. Ask your insurance broker (insurance companies are ramping up their cybersecurity knowledge). National trade groups and local business associations might also have advice and resources. Plus, be sure to check in with your local law enforcement and nearest FBI office (you should at least have contact names and numbers to call in case you experience a cybercrime).

Build your policy. A sound security program begins with policy, and policy begins with C-level buy-in. If you're the boss, then you need to let everyone know that you take security seriously and that your firm is committed to protecting the privacy and security of all data that it handles. Next, you need to spell out the policies that you want to enforce, for example, there shall be no unauthorized access to company systems and data.

Choose your controls. You use controls to enforce policies. For example, to enforce the policy of no unauthorized access to company systems and data, you may choose to control all access to company systems with a unique username, password, and token. To control what programs are allowed to run on company computers, you may decide not to give employees administrative rights on company computers.

At minimum you will want to use three basic security technologies: anti-malware software that will prevent malicious code from being downloaded onto your devices; encryption software that will render data on stolen devices inaccessible; and a two-factor authentication system so that something more than just a username and password is required to gain access to your systems and data.

Deploy controls and make sure they work. For example, you should have a policy that prohibits unauthorized software on company systems; one of your controls will be anti-malware software that scans for malicious code. Not only do you need to install this and test that it doesn't interfere with normal business operations, you also need to document the procedures you want employees to follow when malicious code is detected.

Educate! Your employees need to know more than just the company security policies and procedures. They also need to understand why these are necessary. This means investing in security awareness and education, which is often the single most effective security measure you can implement. Be sure to educate everyone who uses your systems, including executives, vendors, and partners. And remember that violations of security policies must have consequences. Failure to enforce policies undermines the whole security effort.

Further assess, audit, test. Cybersecurity for any business, large or small, is an ongoing process, not a one-time project. You should plan on re-assessing your security on a periodic basis, at least once a year. To stay up-to-date on emerging threats, review security news on a regular basis by subscribing to websites like WeLiveSecurity.com, KrebsOnSecurity.com, and DarkReading.com.

You may need to update your security policies and controls more than once a year depending on changes to the business, such as new vendor relationships, new projects, new hires, or employees departing (for example, making sure that all system access is revoked when anyone leaves the company). Consider hiring an outside consultant to perform a penetration test and security audit to find out where your weak points are and address them.

The current wave of cybercrime is not going to end any time soon, so you need to make an ongoing good faith effort to protect the data and systems that are the lifeblood of today's small business.