

# A HACKER'S DREAM

Small companies can be particularly vulnerable to Internet crimes

MARK ANDERSON | STAFF WRITER

Small-business operators who assume they are too small to be interesting to cyber criminals are missing a critical point, computer-security experts say: They may be more attractive because they are easy targets.

A large corporation typically will have an information-technology team making sure all systems are secure. A lot of small businesses do little more than plug in a computer and connect to the Internet — until something goes wrong.

A survey done last year by computer security firm Symantec Corp. found 42 percent of small- to medium-sized businesses had lost confidential or proprietary information.

"If you are thinking that you are not going to get hacked, you are mistaken," said Penny Leavy, president of Sacramento computer security company HBGary Inc. "It is not a question of whether you are a target, it is a question of when."

## Security steps

Security experts say these are some of the first steps for a small business to secure computer networks:

- Install or activate firewalls on individual computers
- Install and use anti-virus programs.
- Make sure the entry-point to your network, such as a router, also has a firewall.
- Develop a protocol for ensuring security of sensitive information.
- Train employees to spot dangerous email links and follow safe Internet practices.
- Change passwords regularly.
- Ensure that any agreements with service providers spell out what happens if your system goes down or is attacked.

A company related to HBGary, called HBGary Federal, was itself hacked by a notorious group known as Anonymous earlier this year. While Anonymous didn't get inside HBGary's corporate computer servers or systems, the anarchistic network of hackers was able to breach a shared HBGary Google mail server account.

Anonymous launched the attack after the former president of HBGary Federal told TV news shows the company was about to identify ringleaders of the group.

Anonymous was able to use social media

Nearly all people and companies are adapting powerful new equipment and technology at an ever-quicken pace, "and sometimes it is faster than people can develop security for it, so you need to stay updated on all the security features," she said.

The complexity of devices, systems and connectivity is a growing issue in security.



Thor Severson, co-owner of CMIT Solutions of Sacramento, holds a disk that his firm erased for security reasons.

clues and likely reverse encryption programs to get into the email account, which then posted thousands of emails online, including some that suggested the company was proposing to perform dirty tricks on behalf of potential clients.

## TESTING THE SYSTEM

Getting hacked is one way to test the security of a computer network, said Thor Severson, co-owner of CMIT Solutions of Sacramento. CMIT does computer and security work for businesses.

CMIT, like a lot of computer security companies, conducts security audits by actually trying to hack into the client company.

"For businesses, there are — or should be — two major concerns. They are cyber crime and disaster recovery," Severson said.

When a business seeks a security audit, CMIT's employees "send in the gremlins," Severson said. "I would say usually — if not always — we can penetrate their firewalls."

And if the computer security firewalls prove to be robust, well, CMIT's hackers go after the people in the company.

"A lot of security from a technology standpoint is also about people. There is

a lot of human stuff you need to be aware of," he said.

One classic way into a secure environment is a modern equivalent of the Trojan horse.

"We mimic an email from an executive of the company. It looks like it came from the company's email, and it says there has been some server update and we need their passwords and codes," Severson said. "You would be surprised how often people send it."

Indeed, part of any security plan involves training of employees, experts said. That includes teaching workers the most basic principles — like the need to change passwords.

"Most security starts on the inside of the system and not the outside," said Yasar Chaudhary, owner of Computer Experts in Sacramento. "A lot of the users inside of the environment are not being educated and not being careful about what the click on."

## REMOTE ACCESS A RISK

While HBGary got hacked because it earned the ire of Anonymous, most companies get hacked because they have

## BIZ SAVVY

# Social media promotion needs a plan

Campaigns should be organized, engaging, meaningful and fun

Thinking about launching a social media program?

Start with a plan. We've all heard the saying, "if you fail to plan, you plan to fail." Yet that is exactly what most companies do when

it comes to social media: They fail to plan.

You wouldn't launch an advertising campaign without planning. And you certainly wouldn't launch a public relations program without planning. Yet somehow many businesses, especially small businesses, launch social

media programs without a plan. So, before you ask your intern or simply the person on your staff with the most free time, to start posting, blogging and tweeting on your behalf, follow these guidelines to get your program off to a successful start.

**Hire a professional:** You wouldn't put your advertising budget into the hands of an intern, so why would you put your brand there? With social media, your brand voice is on display for all of the world to see, so be sure your 'voice' is a true reflection of your brand and in the hands of a true communications professional.

**Develop an integrated plan:** How will your social media program enhance and integrate with your current marketing efforts? For a program to be successful, it must augment your overall marketing program in a meaningful and strategic way.

**Create a content calendar:** Whether you post, tweet or comment every day or a few times a week, you need to have meaningful content to share. Social media should be organic, authentic and real-time, but as a company, you should

HAMMOND | PAGE 13

## JUST THE FACTS

### Soft market continues

Jobs rise slightly but hours worked and compensation dip for small business from April to May.

Employment (+45,000 jobs): **+0.2%**  
Average monthly hours worked (107.9 hours): **-0.13%**

Average monthly compensation (\$2,624): **-0.14%**

Source: Intuit Small Business Employment Index, based on small businesses with fewer than 20 employees that use Intuit Online Payroll

HACK | PAGE 13