FireEye™

White Paper

# Big Threats for Small Businesses

## Five Reasons Your Small or Midsize Business is a Prime Target for Cybercriminals

# Contents

# Introduction

Your business could be one mouse click away from closing its doors forever. That's the conclusion of a 2012 study by the National Cyber Security Alliance, which found that 60 percent of small firms go out of business within six months of a data breach.[1] Cyber attacks are growing more sophisticated and, more often than not, target small and midsize businesses (SMBs). One unlucky click—a malicious email attachment, a link to a legitimate but compromised website—could result in a costly data breach that drains your bank account and customer trust.

Cybercriminals know there's nothing small about SMBs. In addition to creating 64 percent of net new jobs in the U.S.[2], these economic mainstays account for 54 percent of all U.S. sales and about half of all private-sector payrolls.[3]

Given their vital role in the economy, it's no surprise that the smaller firms face a growing tide of cyber attacks. SMBs aren't just targets—they're cybercriminals' top targets. According to the Verizon 2013 Data Breach Investigations Report, small and midsize businesses suffered data breaches more often than larger firms.[4]

"The 'I'm too small to be a target' argument doesn't hold water," the Verizon report states. "We see victims of espionage campaigns ranging from large multi-nationals all the way down to those that have no staff at all."[5]

A New York mannequin maker learned that lesson the hard way in 2012 when it lost $1.2 million within a matter of hours through a series of fraudulent wire transfers. Cybercriminals breached the 100-employee firm and got its online banking credentials. The company's anti-virus (AV) software never detected anything amiss.[6]

The cost of data breaches can devastate a small or midsize business. According to the Ponemon Institute, data breaches cost U.S. companies $5.4 million per breach on average. That amounts to $188 per stolen record.[7] And that figure doesn't include potential liability issues for the target or the incalculable damage a data breach can wreak on a business' reputation.

Business disruption alone can cost more than $937,000 per breach, the Ponemon Institute estimates.[8] That figure might be bearable for a large enterprise, but would damage most SMBs.

This paper explains targeted attacks and examines five reasons cyber attackers are aiming at small and midsize businesses.

[1] National Cyber Security Alliance. "America's Small Businesses Must Take Online Security More Seriously." October 2012.

[2] U.S. Small Business Administration. "Small Business GDP: Update 2002-2010." January 2012.

[3] Ibid. "Small Business Trends." Nov. 2013.

[4] Verizon. "2013 Data Breach Investigations Report." May 2013.

[5] Ibid.

[6] Sarah E. Needleman (The New York Times). "Cybercriminals Sniff Out Vulnerable Firms." July 2012.

[7] Ponemon Institute. "2013 Cost of Data Breach Study: Global Analysis."

[8] Ibid.

# Today’s Attacks Target Small and Midsize Businesses

News headlines tend to highlight wide-scale attacks against large enterprises, spectacular attacks that hit millions of customers. But most attacks actually target small and midsize businesses. And in relative terms, these attacks often are much more costly to smaller targets.

Unlike the broad, scattershot attacks of the past, today’s cyber assaults are well funded, well organized, and laser focused. The new generation of attacks, including advanced persistent threats (APTs), are focused on acquiring something valuable—sensitive personal details, intellectual property, authentication credentials, insider information, and the like.

Cyber threat actors often lay the groundwork with early reconnaissance. So they know what to look for, where to look, and all too often, the weak links in your cyber defenses.

From there, each attack often cuts across multiple threat vectors—Web, email, file, and mobile—and unfolds in multiple stages. With calculated steps, malware gets in, signals back out of the breached network, and gets valuables out.

Adding insult to injury, cybercriminals often use compromised SMB networks to launch attacks against other targets. As many as 30,000 websites are infected every day, according to one estimate—and 80 percent of those belong to legitimate small businesses.[9]

Targeting small and midsize businesses makes more sense than it might seem. Cybercriminal groups are ruthlessly efficient. They want the biggest bang for their buck, which often means the SMB segment. The following sections outline five reasons that make small and midsize businesses especially inviting targets.

### Reason No. 1: Your data is more valuable than you think

Most businesses have information they want to keep secret. It might be customers’ credit card numbers. It could be employees’ personal data. Or as in the case of the mannequin maker, it might be something as valuable as the keys to the business banking account.

The question isn’t whether cybercriminals are targeting your business, but which ones—and what they’re after.

In addition to having valuable data of their own, most SMBs do business with larger companies. Often this includes deep ties into partners’ computer systems as part of an integrated supply chain or access to their sensitive data and intellectual property.

Think of it as six degrees of separation for business. Even if you’re not the ultimate target—and even if your direct partners aren’t—only a few hops separate you from a valuable target.

“It might not be your data they’re after at all,” the Verizon report states. “If your organization does business with others that fall within the espionage crosshairs, you might make a great pivot point into their environment.”

You might think of yourself as a small fish, but you’re connected to bigger fish.

[9] Alastair Stevenson (V3). “Hackers target 30,000 SME websites per day to spread malware.” June 2013.

## Reason No. 2: Cyber attacks offer low risk and high returns for criminals

The Internet has connected the globe in ways barely conceivable just a few decades ago. It has opened up remote markets, uncovered lucrative niches to serve, and created brand new ways of doing business.

The dark side of this progress: the Internet has also made attacks possible from anywhere in the world. Attackers are rarely caught, let alone punished. Advanced malware typically resides in infected systems for weeks, even months, before common security tools detect it.[10] Some malware quietly cleans up after itself after exfiltrating data to make a clean getaway.[11] And in some cases, attackers are even sponsored by their home government.[12]

Those factors are amplified when it comes to SMBs, which are usually less able than their larger counterparts to detect and counter advanced threats. With much to gain and little to lose, cyber attackers have strong incentives to attack.

## Reason No. 3: You're an easier target

Small and midsize businesses are facing the same cyber threats as large enterprises, but have a fraction of the budget to deal with them. More than 40 percent don't have an adequate IT security budget, according to a November 2013 survey by the Ponemon Institute.[13]

Unlike big corporations—with dedicated roles for chief information security officer, chief information officer, and the like—the typical IT director at a small or midsize business wears many hats. Only 26 percent of small and midsize businesses in the Ponemon survey were confident their firm has enough in-house expertise for a strong security posture.[14]

Most small businesses cannot afford layered "defense-in-depth" security employed by large enterprises. And even if they could, most of these defenses are futile anyway. (See Reason No. 5: "Most SMB security tools are no match against today's attacks.")

Likewise, many smaller companies lack strong security procedures and policies. Only 36 percent of small business owners have data security policies, according to a September 2013 survey sponsored by Bank of the West.[15]

Most cyber attackers follow the path of least resistance. In many cases, this means targeting the very businesses that can least afford to be hit.

## Reason No. 4: Many SMBs have their guards down

The statistics are clear: a small or midsize business is more likely—not less—to face a cyber attack compared with large enterprises.

And yet nearly 60 percent of small and midsize businesses in the Ponemon survey don't consider cyber attacks a big risk to their organization. And 44 percent don't consider strong security a priority.[16]

[10] Verizon. "2013 Data Breach Investigations Report." May 2013.

[11] Lucian Constantin (IDG News Service). "Flame authors order infected computers to remove all traces of the malware." June 2012.

[12] U.S. Department of Defense. "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013." May 2013.

[13] Ponemon Institute. "The Risk of an Uncertain Security Strategy Study of Global IT Practitioners in SMB Organizations." November 2013.

[14] Ibid.

[15] Harris Interactive. "Fighting Fraud: Small Business Owner Attitudes about Fraud Prevention and Security." September 2013.

[16] Ibid.

Despite a growing tide of cyber attacks, 77 percent of SMBs believe that their company is safe from cyber attacks, "showing that some small businesses are operating under a false sense of security."[17]

Many businesses assume that they don't have anything worth stealing (see Factor No. 1: Your data is more valuable than you think). Others are unaware of the volume and sophistication of today's attacks.

In either case, the effect is the same: the business remains vulnerable. As the Verizon report puts it:

> *Am I a target of espionage? Some may already know the answer to this question by firsthand experience. Many others assume they aren't or haven't thought much about it. Despite the growing number of disclosures and sometimes alarmist news coverage, many still see espionage as a problem relevant only to the Googles of the world. Unfortunately, this is simply not true.*

### Reason No. 5: Most SMB security tools are no match against today's attacks

The defenses most SMBs have in place today are ill equipped to combat today's advanced attacks. Firewalls, next-generation firewalls, intrusion prevention systems (IPS), AV software, and gateways remain important security defenses. But they are woefully ineffective at stopping targeted attacks.

These technologies rely on approaches such as URL blacklists and signatures. By definition, these approaches cannot stop dynamic attacks that exploit zero-day vulnerabilities. If an IPS or AV program does not have the signature of a new exploit, it cannot stop it. When highly dynamic malicious URLs are employed, URL blacklists do not cut it.

Most defenses stop known attacks. But they are defenseless against unknown advanced targeted attacks.

## Recommendations

Most cyber attackers are rational. Attackers have strong incentives to target your systems, with little potential consequence. Given the value of your data, your business cannot afford to ignore the threat—or waste time and money on ineffective defenses.

Here are three key steps toward shielding your business from the growing scourge of data breaches.

### Assume you're a target

Cyber attacks against small businesses rose 31 percent in 2013 versus the year before, making them the fastest-growing group of targets.[18]

Your data is valuable. And you likely have ties to bigger, high-profile business partners. Given that today's advanced attacks can easily bypass most security tools, you may have been breached and not yet know it.

By assuming that you are in cyber attackers' crosshairs, you can better prepare yourself against the inevitable attack.

[17] National Cyber Security Alliance. "America's Small Businesses Must Take Online Security More Seriously." September 2013.

[18] Brian Moran (Small Business Edge). "Protecting Your Business From Hackers and Cyber Crimes." November 2013.

### Identify your most value assets and links

You would never hire bodyguards and forget to tell them whom they are supposed to be protecting. In the same way, defending your systems starts with identifying your most valuable assets.

That step might be trickier than it sounds. Information that seems ordinary to you—say, the name of a business contact's executive assistant—could help cyber attackers forge a spear-phishing email that compromises a vital partner.

Identify potentially valuable data and how it could be vulnerable to well-funded, highly organized attackers. That crucial step will help spot the weakest links in your security system and highlight what you need to do to protect your assets.

### Deploy a security platform capable of identifying and blocking today's attacks

A widening gap between threat actors' offensive abilities and badly outdated defenses has left organizations more vulnerable than ever. Today's attacks exploit previously unknown, zero-day vulnerabilities, easily bypassing signature- and reputation-based defenses. And file-based sandboxes, touted by legacy vendors as their fresh approach to security, are constrained by many of the same flaws as traditional security products.

Even with constant updates, standard security products —traditional and next-generation firewalls, IPS, gateways, and AV software—cannot keep up with today's fast-moving, ever-evolving threats. By the time most products can update their databases of known malware and high-risk Web addresses, attackers have fashioned new, undetectable attacks.

SMBs must take a radically different approach. They need a security platform that can detect and block both known and unknown threats with real-time, coordinated security.

To learn more about advanced attacks and how FireEye can help protect your small or midsize business, visit www.FireEye.com.

### About FireEye, Inc.

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors, including Web, email, and files and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,300 customers across more than 40 countries, including over 100 of the Fortune 500.

© 2013 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. – WP.SMB.EN-US.122013