A BUSINESS OWNER'S GUIDE TO CYBERSECURITY

Protect Your Business with a Layered Security Approach

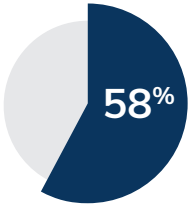
VIPRE®

The True Risk of Cyberattack for SMBs

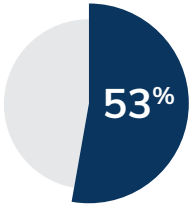
You've probably read about the frequent and high-profile data breaches of enterprise companies and large government agencies. But does the relative lack of news coverage involving small and medium-sized businesses (SMBs) mean that, for them, the cybersecurity risk is much smaller?

Many business owners believe that their companies don't provide valuable-enough targets for cybercriminals because they don't have thousands of employees or millions of customers. They may be lulled into thinking that even if they do experience a cyberattack, it won't be severe enough to halt operations or impact profitability.

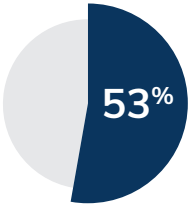
The reality, however, is quite the opposite. SMBs have information and credentials that are indeed valuable for cybercriminals, including: employee and customer records, access to business financial information including bank accounts, and access to larger companies and their networks through the supply chain. In fact,



Data breach victims that are small businesses[1]



Midmarket companies (250-499 employees) that have experienced a data breach[2]



Small businesses that would be unprofitable within one month if they permanently lost access to essential data[3]

It's clear that SMBs are far from immune to cyberthreats. This ebook can help you understand how and where cybercriminals are likely to strike and how to protect your business from cyberattack using a layered security approach.

1. "2018 Data Breach Investigations Report," Verizon, 2018.
2. "2018 Security Capabilities Benchmark Study," Cisco, 2018.
3. "2017 State of Cybersecurity Among Small Businesses in North America," Better Business Bureau, 2017.

CAN YOU KEEP THE DOORS OPEN AFTER AN ATTACK?

66%

of IT managers in businesses of 50 to 1,500 employees say their company could close following an attack

44%

say the company would close for a day

22%

say the company would go out of business

Source: VIPRE, Managing Cyberattacks Survey, 2017

The Top Ways That Cybercriminals Can Slip Into Your Business

To protect your business, you need to understand where cybercriminals are most likely to attempt an attack. There are three vectors (paths or means) that cybercriminals can use to get into your business electronically. Of course, these vectors are also important, and sometimes essential, parts of your business operations. An attack that renders any or all of these areas unusable for a period of time could be devastating.

EMAIL

The most common attack vector, email is the starting point for malware, phishing, and other types of attacks (more on what these are later).

ENDPOINTS (computer equipment and smart devices)

Would-be attackers can exploit any potential endpoint via malware, bots, viruses, spyware, and more. An endpoint is anything that connects to a network, including: desktop computers, laptops, smart phones, tablets, point-of-sale (POS) terminals, and other devices.

NETWORK

Any network that connects to the internet and is used by your employees (e.g., your company's network, the free WiFi at a coffee shop, customer networks) can be used by cybercriminals to attack your business.

WILL YOUR EMPLOYEES OR SERVICE PROVIDERS FALL FOR THIS?

Business email compromise (BEC) attacks target companies with scam messages intended to extract information or money from unknowing recipients.

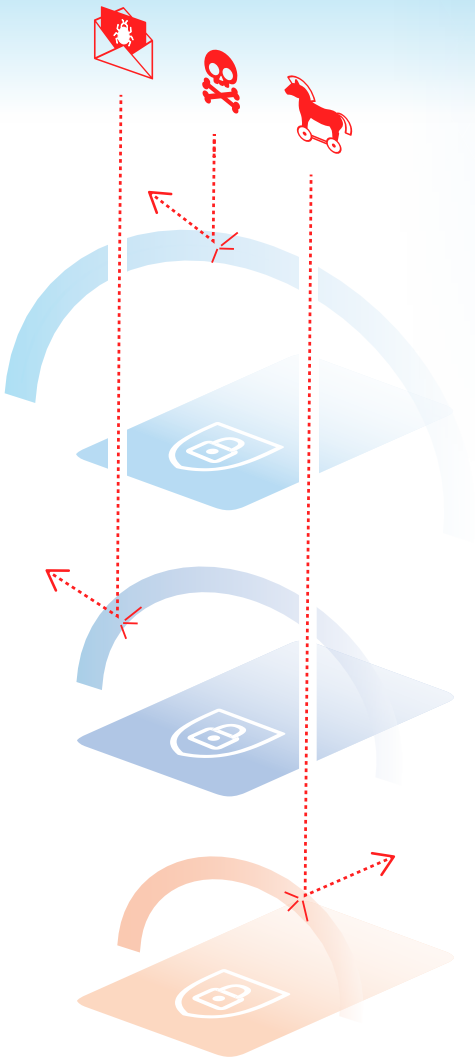
EXAMPLE 1

A fraudulent email is sent from someone pretending to be your company's CEO to your outsourced human resources (HR) provider. Without realizing that he or she is being scammed, the HR provider sends personal employee data to the scammers, which is then used to create phony tax returns and fraudulent IRS refunds.

EXAMPLE 2

Someone pretending to be a company executive sends an email to an employee requesting a wire transfer be sent to a vendor or supplier immediately. The employee wires funds to the fake vendor's account.

Layers of Security Thwart Attacks



No one keeps cash in an open box just inside a company's front door. That's because all a would-be thief would have to do is unlock or break the door. Instead, businesses use layers of physical security to hide and protect their assets. If a criminal gets through one layer, there are other mechanisms that can still prevent theft or destruction.

The same goes with protecting your business' digital assets. One virtual "lock" won't keep out every intruder. Instead, you need layers of effective cybersecurity measures that make it difficult for an attack to slip past all of your defenses.

To protect your business, your customers' and partners' data, and your technology investment from harm, you need to make sure you have all three attack vectors protected with layers of defense. Those layers include a business-grade firewall for security of your network, endpoint security, and email security. Threat intelligence works with all three layers to keep them updated on the latest threats.

Network Security

- Intelligent firewall
- Threat intelligence
- Sandboxing
- IDS/HIPS

Email Security

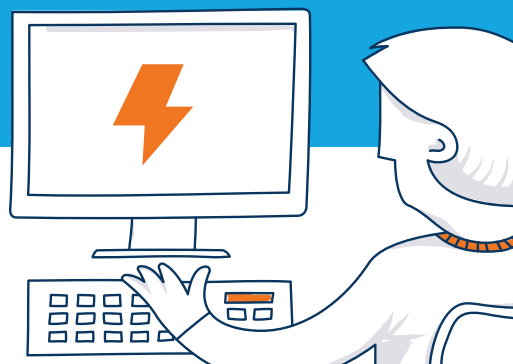
- Anti-virus, spam and phishing
- URL protection
- Microsoft macros
- Bulk and grey mail
- DLP encryption

Endpoint Security

- Device control
- Active protection
- Machine learning and Artificial Intelligence
- DNS, URL filtering and packet inspection
- Email anti-spam

MALWARE EXPLAINED

The term malware, coined from the combination of malicious and software, is any software that is intentionally designed to gain access to, make malicious use of, or damage a computer or device. There are many different types of malware including: viruses, worms, Trojans, ransomware, fileless, adware, spyware, and more.



What You Should Know About Endpoint Security

Chances are good that much of your business happens on the go these days. You and your employees may be logging into the systems that help you run your business and serve customers from just about anywhere, on any device that connects to the internet, whether it's a tablet within your store, a smartphone at a job site or a laptop at your clients' business locations.

While network security will hopefully be in place for the networks you use, you need more layers of protection. This next layer is at the endpoint level, so that you can protect against a cybercriminal trying to take advantage of your company's or employees' devices to infiltrate your business.

Endpoint security solutions protect your business from emerging threats such as viruses, Trojans, rootkits, exploits, spyware, malicious websites, phishing attacks, ransomware and more. For the greatest protection as well as ease of use, look for a solution that provides:

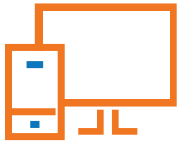
Sophisticated detection methods that go beyond signature-based antivirus detection to help protect you against both known and emerging threats

Advanced machine learning for behavioral analysis

Up-to-date threat intelligence

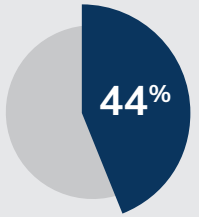
Dashboards and alerting that give you a clear view of what's happening

Rapid deployment and ease of management

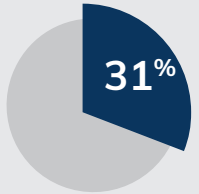


Support for the operating systems and devices your business relies on

CAN YOUR BUSINESS AFFORD A DATA BREACH?



Small businesses that report being the victims of data breaches



Small businesses that spent more than $50,000 to resolve a customer data breach

Source: "Small Business Payments Spotlight," Bank of America, 2017.

What You Should Know About Email Security

Did you know that 92 percent of malware is delivered via email?[4] And that phishing emails continue to be a tried-and-true attack method to obtain sensitive information or infect a device with malware?

Cybercriminals are finding increasingly sophisticated ways to use email to commit malicious acts against you, your employees and your company. That's why you need another layer of security focused on email that protects your business against malware infections, phishing, spam and accidental or malicious data loss via email.

For a powerful and easy-to-manage solution, look for email security that provides:

- Multiple levels of scanning as well as advanced machine learning to identify both known and emerging email-based threats
- Virus, spam, and phishing detection and protection against unwanted or malicious emails
- Up-to-date threat intelligence
- Real-time behavioral sandboxing to isolate testing for malware from the rest of your environment
- Support for any email client or server
- Centralized management

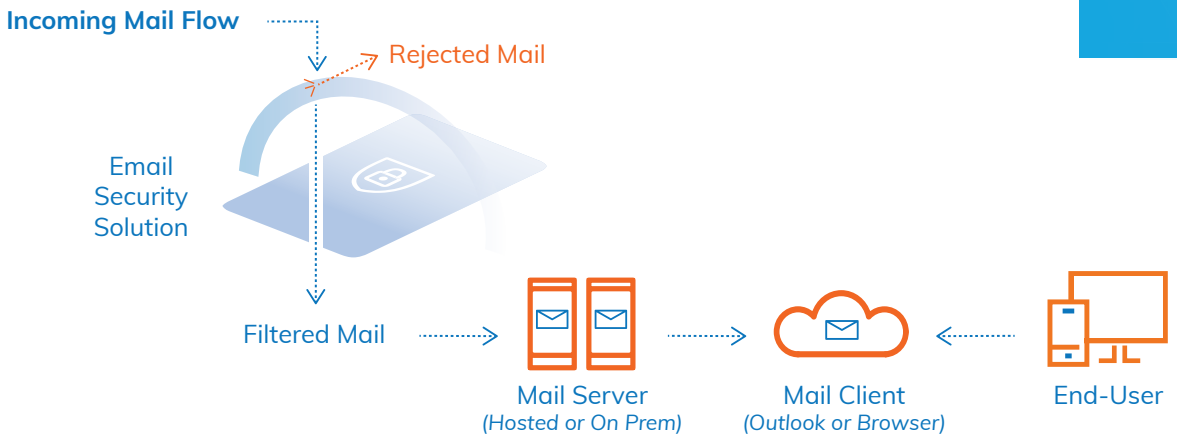
TO CATCH A PHISH

Can your employees spot a phishing scam?

Phishing is "the crafting of a message that is sent typically via email and designed to influence the recipient to 'take the bait' via a simple mouse click. That bait is most often a malicious attachment but can also be a link to a page that will request credentials or drop malware."

It's one of the oldest types of cyberattacks, dating back to the 1990s, and it's still one of the most widespread, with phishing messages and techniques becoming increasingly sophisticated.

Source: VIPRE, Managing Cyberattacks Survey, 2017.



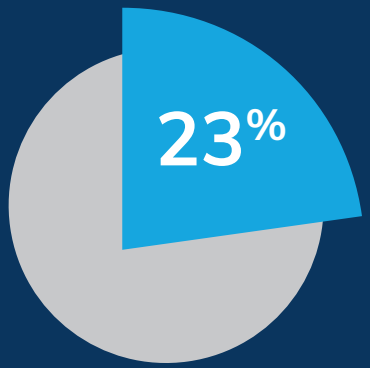
4. "2018 Data Breach Investigations Report," Verizon, 2018.

What You Should Know About Threat Intelligence

Like everything else that's digital, change is a constant when it comes to cyberthreats. Cybercriminals adapt their techniques based on their learnings from successful attacks and unsuccessful attempts. That's why thousands of new malware variants are released every day, fine-tuned for greater success and to evade detection.

How can your layered security measures possibly keep up? The answer is threat intelligence. Threat intelligence, according to the SANS Institute is "the set of data collected, assessed and applied regarding security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators." It's the collective information about the latest techniques and tactics being used by cybercriminals.

Having the latest intelligence helps email and endpoint security solutions better detect and block threats. Choose email and endpoint security solutions from a vendor that offers global threat intelligence services and integrates them with their products.



IT managers at companies with 50 to 1,500 employees who reported cyberattacks happening at a rate of one or more a day.

Source: VIPRE, Managing Cyberattacks Survey, 2017.

Next Steps

How well is your business protected from the onslaught of cyberattacks? Do you have a layered approach to detect and stop attacks that may evade an individual security measure?

More than half (62 percent) of SMBs don't have an up-to-date or active cybersecurity strategy in place.[5] One reason is that many SMBs simply don't have the time, personnel or skills to take on cybersecurity. Outsourcing this critical function to IT and security professionals can help improve your level of protection against threats and speed of response in case of attack.

Regardless of where you are in your cybersecurity efforts, here are some steps you can take to better protect your business against attacks and breaches:

1. Make an honest assessment of your current cybersecurity defenses and the potential risks your company faces if there's a breach
2. Decide whether you can manage cybersecurity in house or whether it would be better to outsource it
3. Implement layered security measures to detect and block attacks
4. Educate employees on cybersecurity threats and best practices

5. "Cyberthreats and Solutions for Small and Midsize Businesses," Vistage, 2018.

About VIPRE

VIPRE is a leading provider of advanced security products purpose-built to protect every major attack vector from today's most costly and malicious online threats. Leveraging decades of proven industry expertise, our award-winning software portfolio includes comprehensive email and endpoint security, along with real-time threat intelligence and the industry's premier sandbox for next-gen malware analysis.

Unlike competitive solutions, VIPRE products are designed to defend against evolving threats without compromising the needs of modern business. We offer flexible cloud configurations for rapid, affordable deployment, plus native mobile interfaces that enable instant threat response—anywhere, anytime. Add in our consistently high ratings from the world's most widely-trusted independent testing labs, and it's no wonder that millions of global users depend on VIPRE for a complete approach to cybersecurity.

To learn more, visit www.VIPRE.com

VIPRE®

VIPRE_2019_EB_BusinessOwnersGuideCybersecurity_0131_US