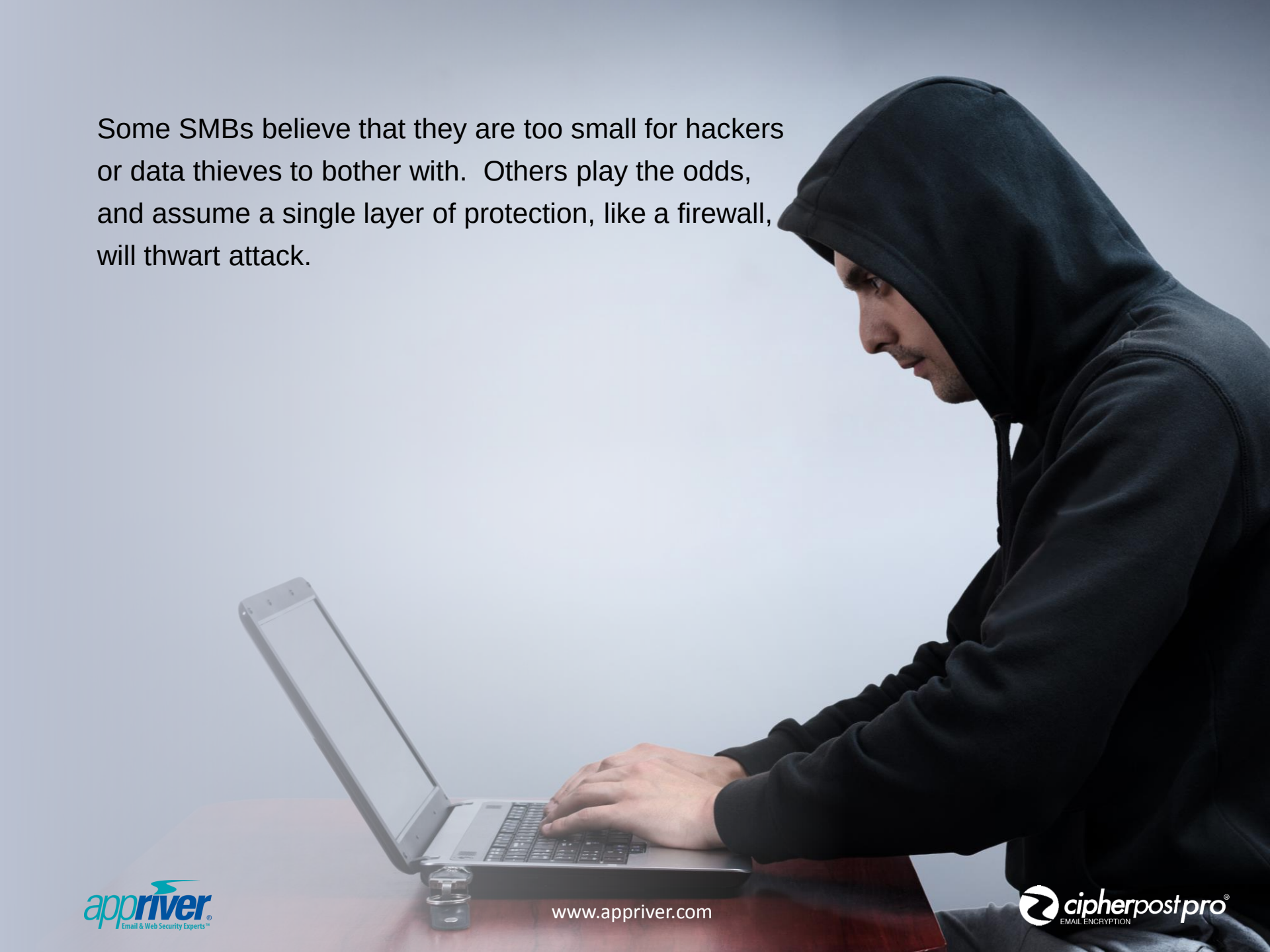

# Understanding Layered Security and Defense in Depth

# Introduction

Cybercriminals are becoming far more sophisticated as technology evolves. Well-publicized security breaches of major corporations are capturing the public's attention, but the truth is that small and mid-sized businesses (SMB) are not immune and can become lucrative targets.

What are "layered security" and "defense in depth" and how can they be employed to better protect your IT resources? Understanding these strategies and how they can be used to improve your security posture is important.

Some SMBs believe that they are too small for hackers or data thieves to bother with.  Others play the odds, and assume a single layer of protection, like a firewall, will thwart attack.



History shows that these are dangerous misconceptions.  SMBs often handle large volumes of personally identifiable information that if found in the wrong hands could have longstanding, damaging impact.

Technology has made it possible for hackers to extend their reach to vast number of potential victims through a wide variety of attack vectors.

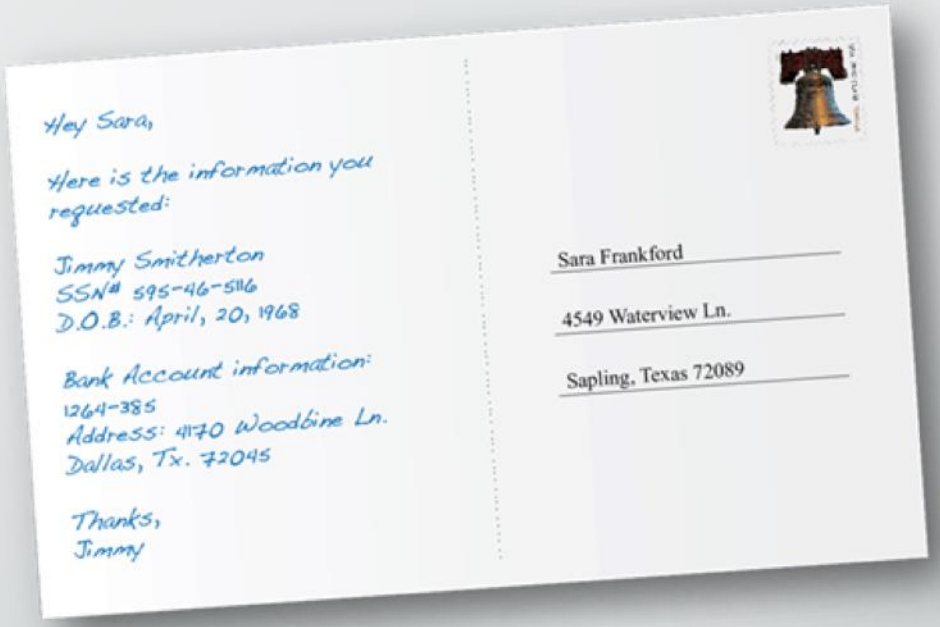
# Delivery Methods…

Today's cyber criminals employ many methods to steal information and money.  And since so many people maintain and rely on email accounts, what better place for cyber criminals to target?

Email-borne attacks come in the form of phishing, spear-phishing, Trojans, malicious attachments, and hidden scripts.  Attack techniques are ever-evolving and adapt with technology in an effort to stay ahead of security professionals—driving malware authors to become very good at what they do.

# Email as a Postcard

In addition to threats from malicious messages, a company's own email can be compromised in transit.  The best way to think about unencrypted email is as a postcard that can be read by anyone.



Based on the growing volume of sensitive information crossing networks daily, regulatory bodies have turned their concerns to ensure messages are protected from unauthorized viewing. The following list includes just some of the requirements that are driving email encryption adoption around the globe:

- EU Data Protection Directive (also known as Directive 95/46/EC)
- Payment Card Industry Data Security Standards (PCI DSS)
- Health Insurance Portability And Accountability Act (HIPAA)
- Sarbanes-Oxley Act (SOX)
- Gramm-Leach-Biley Act (GLBA)

The consequences of violating these and other industry encryption requirements can include fines, incarceration, public embarrassment, loss of business privileges and customer/stakeholder trust.

# Staying Ahead of Threats…

IT security is so often a game of “cat and mouse,” whereby cybercriminals and security professionals are in constant pursuit of one another. The “cat” (or security professional) is unable to definitively claim victory over the “mouse” (cybercriminal) who despite not being able to defeat the cat is able to avoid capture.

Today's threats are not static, predictable or simple.  And the models for distribution can vary from cast-net style malware campaigns to precisely-targeted advanced attacks. No industry or business is immune and that is why all organizational security policies should include defense in depth.

# Layered Security

The idea behind layered security is that there is no “silver bullet” that can make your systems 100-percent safe from attack. The best approach is to have multiple, redundant safeguards in place.

When evaluating your company's security posture, it's critical to understand all points of vulnerability within the organization. Wherever you have a device connected to the Internet, you have a potential entry point for cybercriminals. Here are some vulnerabilities to consider:

**Computers:** Desktops, workstations and kiosks

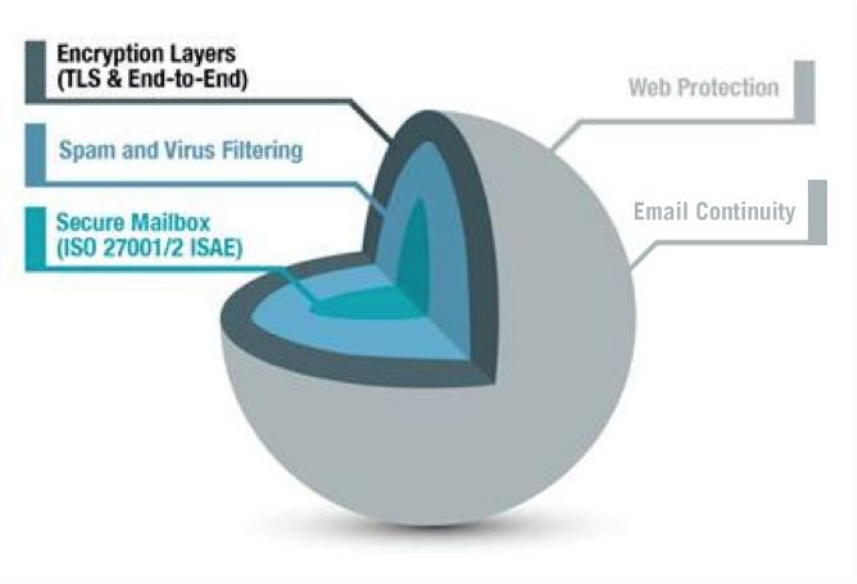
**Mobile devices:** Smartphones and tablets

**Network:** On-premises and/or cloud-based servers

**Users:** Every employee, contractor or visitor who has Internet access

# Layers of Protection

To protect your company and customer information, you need to build security in layers that cover each of the areas where your data is vulnerable



# The Importance of Data Security

Data that is encrypted is unusable to those who do not have the proper decryption keys and means to decrypt.

End-to-end encryption solutions ensure the uninterrupted protection of transmitted data by encoding it at its starting point and decoding it at its destination. Look for vendors that offer encryption solutions that wrap around any existing email infrastructure or application so that your organization does not have to replace existing technology, including email addresses or email programs. Also look for solutions that provide certified email delivery and tracking slips so that authorized individuals may see multiple characteristics about any given message, such as who sent it, who received it and how it was handled, including deletions, forwards and attachment downloads that are time stamped with corresponding IP addresses.