HIGHER STATE
technology

STATE OF SECURITY

An insight into the current threat landscape, who's the target and what you can do about it

# TABLE OF CONTENTS

People work anywhere and everywhere now, from co-working spaces and coffee shops to airport lobbies, using innovative devices, apps and cloud services to reimagine and redefine their workdays.

It's great for productivity and efficiency - but it's stretching network security to the breaking point, creating hidden gaps and vulnerabilities as employees move further away from the traditional 'office'. With most security solutions still focused on protecting employees only while they're on the corporate network, organizations are increasingly at risk for cyberattacks.
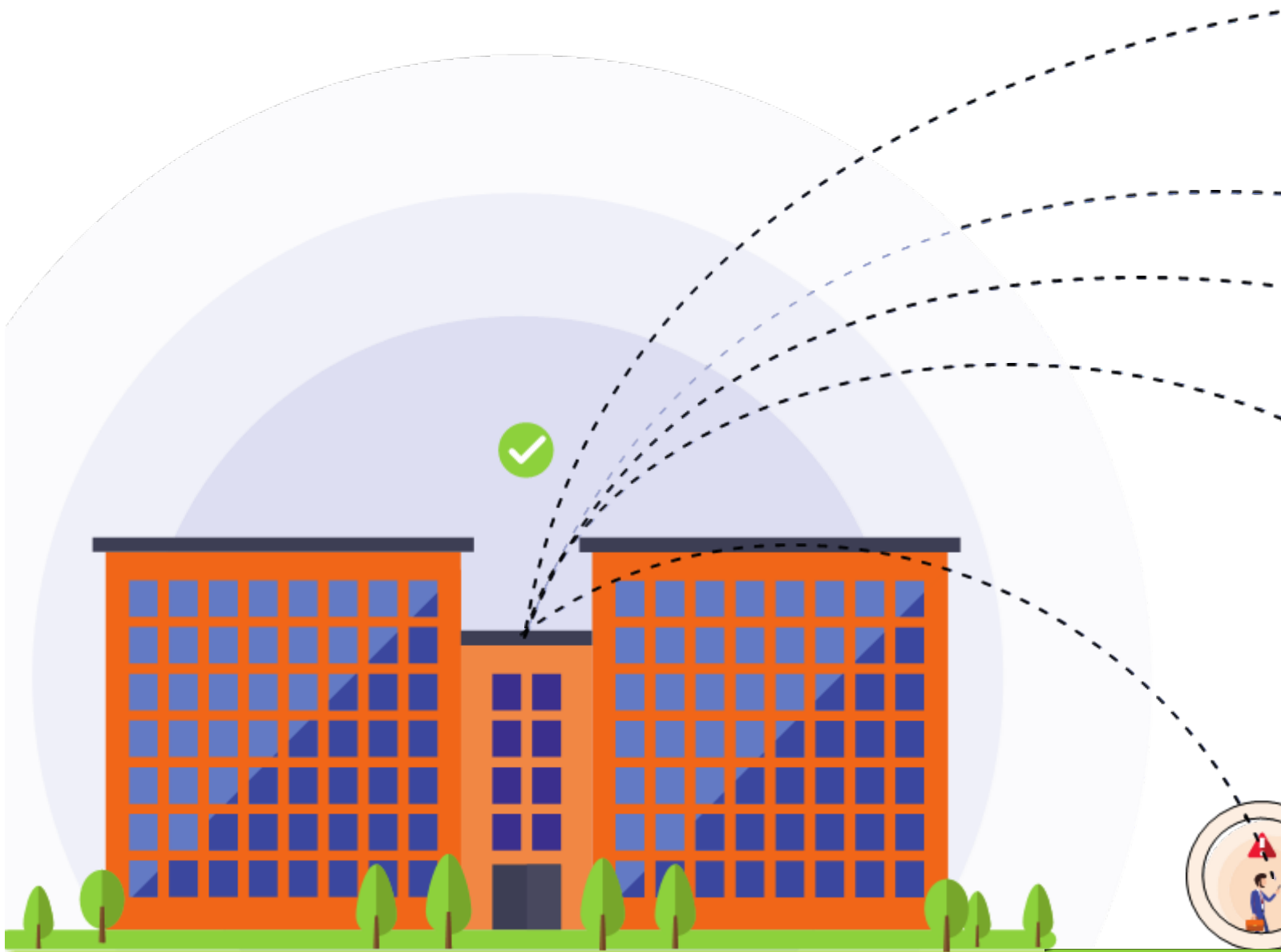
Hackers are paying attention, and they're matching today's technology innovations with maddening creativity of their own. They've graduated from attacks designed to steal data to extortion hacks that lock people out of their data unless a ransom is paid. One of the most frightening advances that **Higher State Technology** is also seeing is 'Exploit as a Service', if you're a criminal with just $200 in your pocket and a little incentive to earn more, your startup cost is less than if you were to open up a coffee stand. So get ready, because current security reviews and surveys say attacks increased by 38% in 2016, and it is predicted they'll continue to grow - in frequency, and in volume.
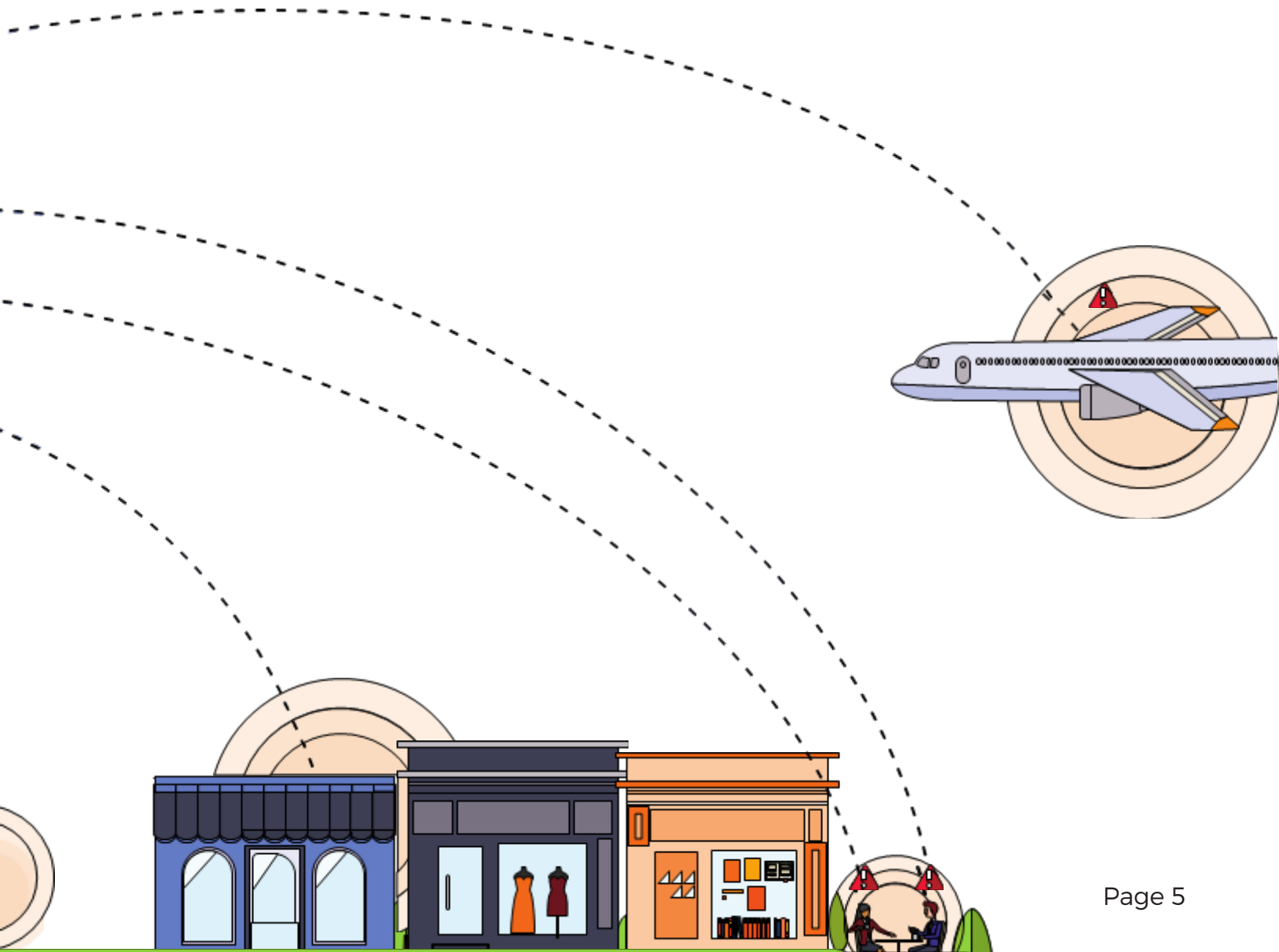
SMB's in the crosshairs

This has resulted in SMB's becoming worthy targets. Today's criminals often gain access into an SMB's network as a means to find an entry point into another more lucrative network (often enterprises), and the SMB is the starting point for such an attack.

50% of SMBs have been breached in the past 12 months

The average total cost of a data breach in the US is $6.5 million

**There are on average between 80 - 90 million cybersecurity incidents per year**

68% of funds lost as a result of a cyber attack were declared as unrecoverable

That's a lot on the line.

There is no single solution to ensure your organizations secure and protected from cyber security attacks. Your business needs to take a multi-faceted approach. Which raises the question... What is your organization doing to block the threat of a breach?

This eBook takes a look at the current threat landscape facing **US** SMB businesses and what you can do about it.

"There are no borders with cybercrime and it's a very big, lucrative business."
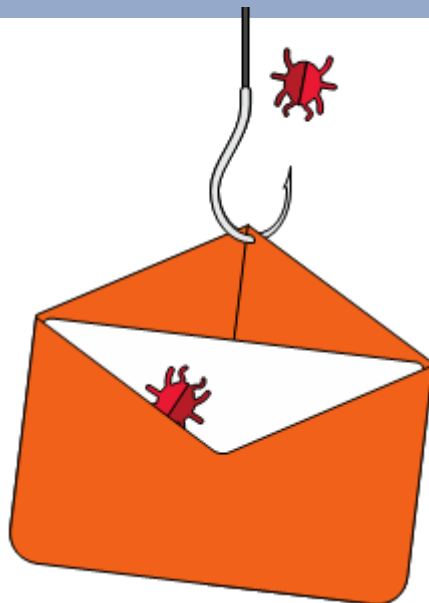
The Current Threat Landscape

Cyber criminals know that businesses are working over-time to secure their environment against threats, which means cyber criminals are working just as hard to find new gaps to exploit.

Exploit Kits 'as a Service'

We mentioned earlier 'Exploits Kits as a Service' are one of the most frightening advances that we are seeing, but what are these exactly? Exploit kits as a Service is a relatively recent business model used by cyber criminals in which they create, manage and sell (or rent) their malicious code to anyone interested. Exploit kits do not require technical expertise and can be bought for as little as $200.
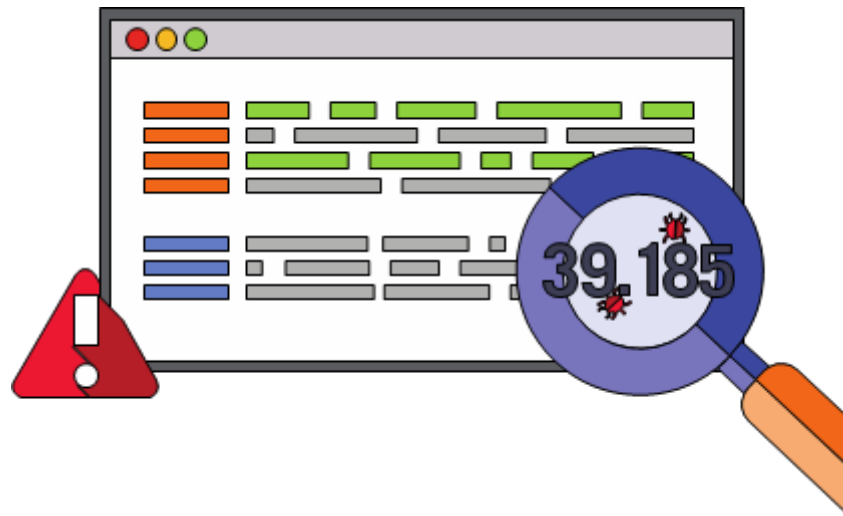
'Blackhole' is a great example of Exploit Kits as a Service, the author is one of the very few that has been caught. As such, we know that he had more than 1000 customers using his kit and was making over $50,000 per month in subscriptions. This is a person that never actually attacked a victim, but instead sold his malicious software to other cyber criminals to use.
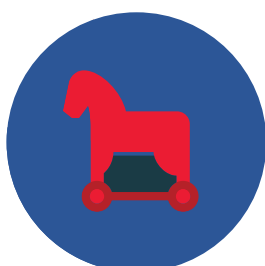
Malware - What is it really?

Short for malicious software, malware is a broad term used to describe a variety of intrusive software. It may be silent, intending to steal data or spy on users without their knowledge, and passively record / obtain sensitive information e.g. passwords to bank accounts. Or it may be designed to cause harm, including sabotage and extortion such as the various forms of cryptolocker that many businesses within United States have experienced.

The various forms of Malware include:
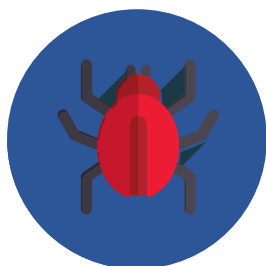
Viruses	**Trojans**	**Worms**	**Bot (Robots)**
Spreads itself from one file to another	Masquerade as harmless until activated	Self-replicate themself through the network	Allow hackers to take control of many computers at a time

The Rise of Malvertising

Malvertising, or malicious advertising is a growing problem. Malvertising purposefully targets reputable websites with high traffic with online advertising to distribute malware with little or no interaction required. In some instances you don't even need to click on an ad to become infected. JavaScript exploits and Facebook scams are the most frequently used attack methods criminals use according to recent research from Cisco.

Typical Malware Workflow

Entry

User clicks on an
email link or
malvert or visits
a compromised
website

Exploit

Initial exploit
probes the users
system for
vulnerabilities

Execution

With an infected
system it is now
identifying what
the infected cost is
to the business.

Infection

Malware is
activated and
communicates
with it's creator to
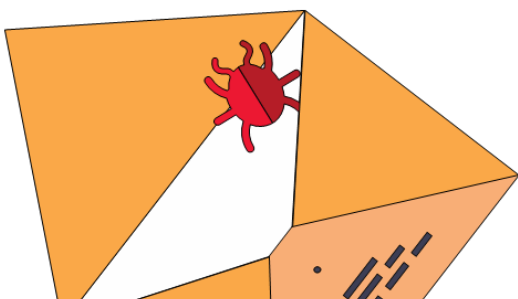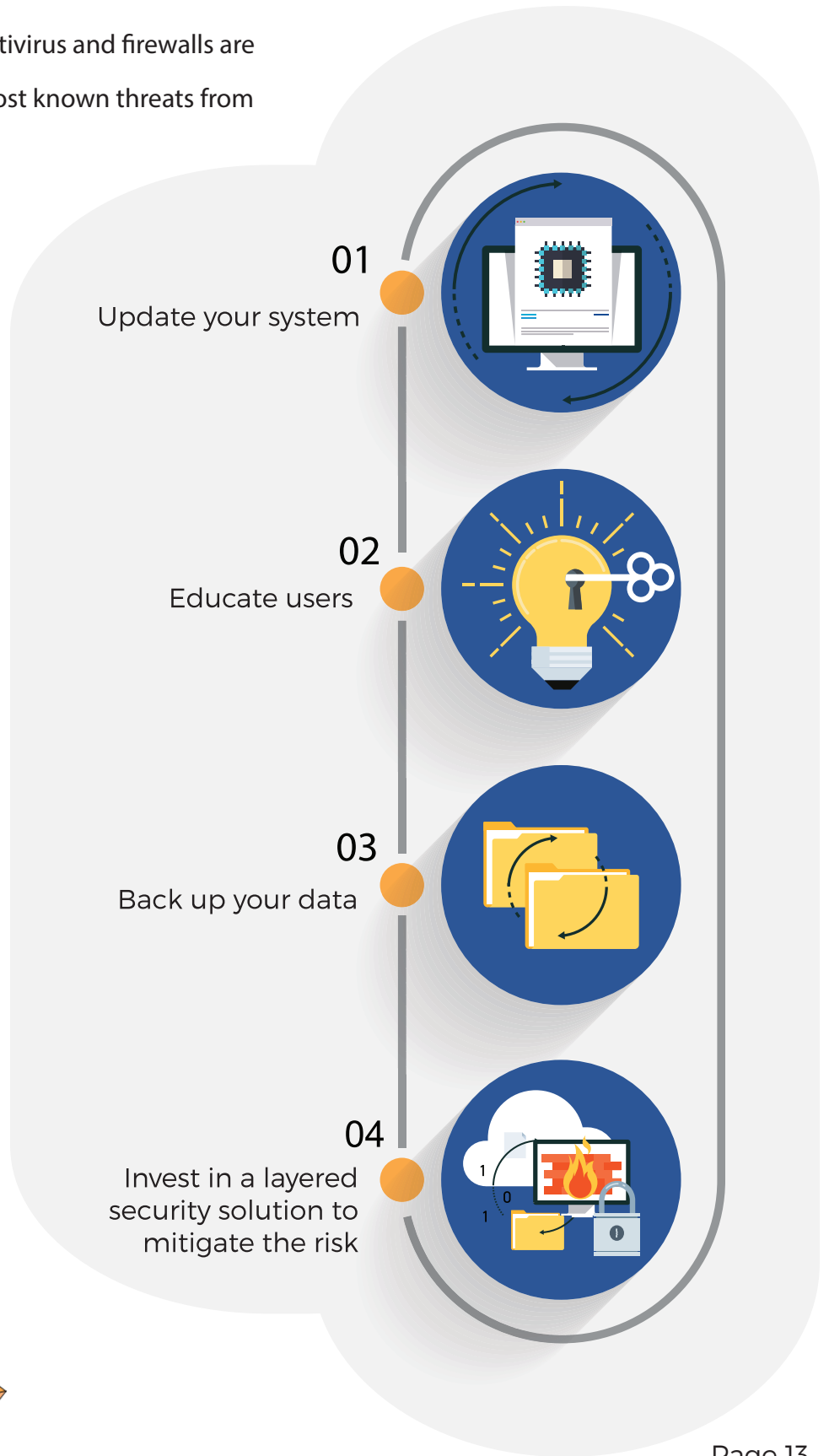start infecting the
system..
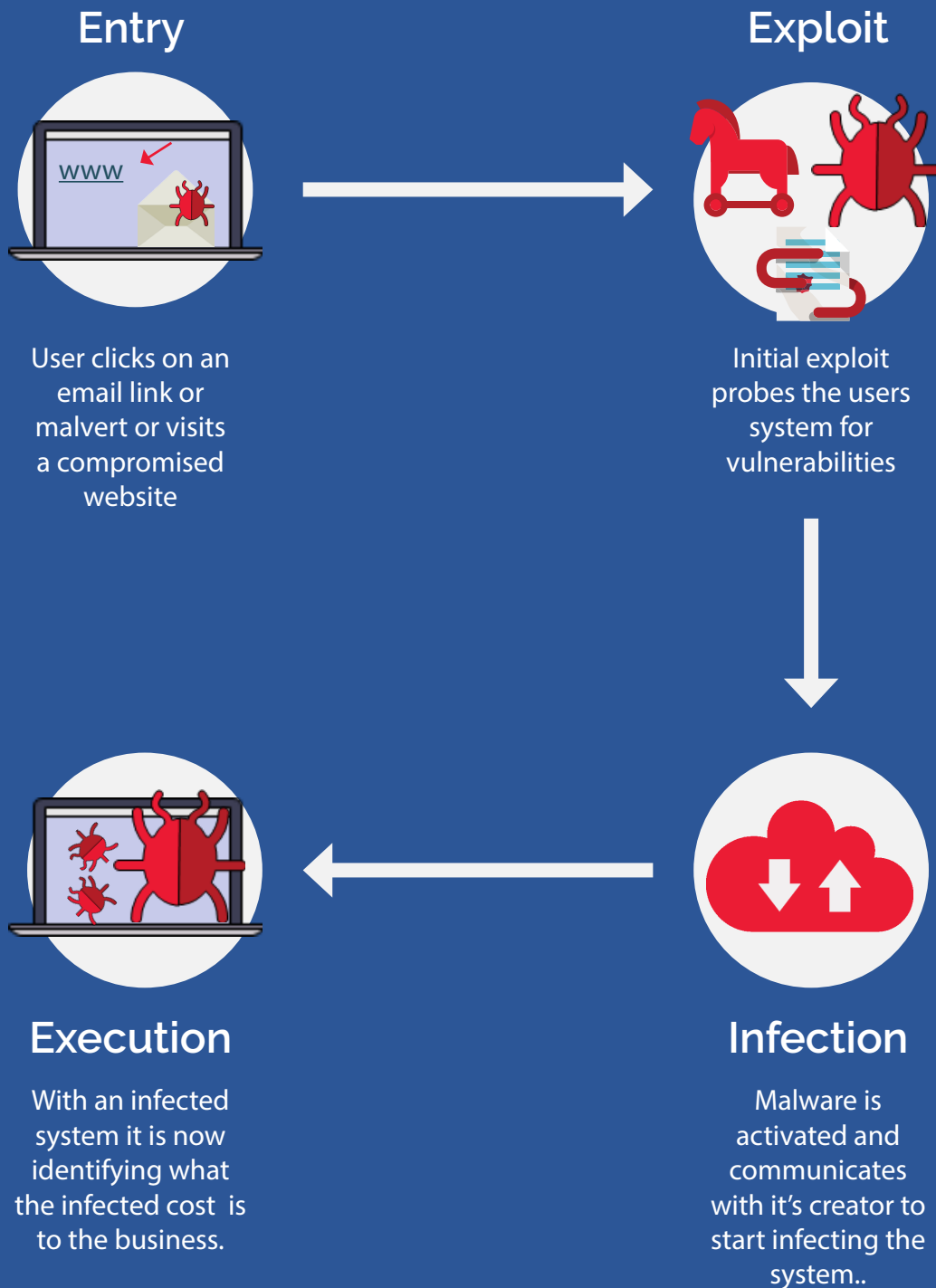
CHAPTER 2

How you can protect yourself

Given these challenges, what's the solution?

To ensure your organizations secure and protected from cyber security attacks. Your business needs to take a multi-faceted approach

The traditional security approach hasn't changed much, and in some ways, that's not a bad thing. Every piece of malware ever created is still out there, and antivirus and firewalls are still important in preventing most known threats from infecting your systems.

However, more than 90% of threats are arriving via the internet and this should be every company's first layer of support.

01
Update your system

02
Educate users

03
Back up your data

04
Invest in a layered security solution to mitigate the risk

Leveraging a secret weapon

Those signature based solutions such as firewalls and antivirus take care of known attacks. But what about the new ones that you can't see coming? To handle these, organizations must move beyond local, reactive intelligence to predictive intelligence based on internet-wide visibility across all geographies and markets. Why? Because hackers use the internet to develop, stage and refine their attacks - and in doing so they leave behind traces like domain names and callbacks that can be analyzed.

Higher State Technology Cyber Security Solution detects and contains advanced internet based attacks *before* they cause wide spread damage. This platform compliments your existing security measures by providing insight into the connections and relationships between networks on the Internet.

This gives you the power to stop advanced threats earlier and extend your network perimeter to protect employees and devices <u>anywhere</u>

Higher State Technology's Cyber Security Solution compliments your existing security measures and stops malicious traffic before it even gets to you.

Internet delivered threats are real and will only continue to grow in volume and complexity. Especially in today's mobile world it is critical for businesses to stay secure when working outside the office. Security implemented at this level provides the power to uncover and block connections to malicious domains inside and outside your corporate network, providing security that moves with your employees.

85% of all organizations (private & government) were successfully breached with Phishing attacks in 2015 alone

Average time to discover a breach is 205 days

71% of data breaches are waged against companies with less than 100 employees

60% of small businesses close within six months of experiencing a data breach

Contact Us

🏠 525 Round Rock West Dr.
Suite C300
Round Rock, Texas 78681
Phone: (512) 900-9478

www.higher-state.com
sales@higher-state.com

Higher State Technology

HIGHER STATE
technology

Higher State Technology provides IT Consulting and our Managed Services offering to keep your critical IT resources secured and operational 24x7.

Our focus is to keep your IT systems operational, available and secure so that you can focus on the everyday demands of expanding your business, managing costs and increasing revenues. We're here to help you realize the productivity gains and ROI you have been expecting from your computer systems all along.

As trusted advisors, we evaluate your technology and support needs and design with the future in mind. Beyond solving your technical problems, we design and enable systems that ensure your network functions optimally and securely to facilitate your business goals.

Higher State Technology, LLC (www.higher-state.com) provides outsourced, enterprise-grade level Managed IT Services and Support and serves as a company's IT Operations Center to include network and security operations. With a diverse and talented team and the industry's leading partner-vendors, HST offers SMBs affordable and scalable solutions for best practices, security, infrastructure, voice/unified communications, network administration and collaboration. HST is author of a proprietary Strategic IT Roadmap process and project plan that aligns a company's business model and growth plans to timing of IT investments, scheduling, budgeting and financing. We are seasoned business builders who can help you leverage technology for business performance improvements, revenue acceleration and margin improvements.