KnowBe4
Human error. Conquered.

# REPORT
## The 2017 Endpoint Protection Ransomware Effectiveness Report

What started out as a nuisance written by a handful of amateur hackers has turned into the most lucrative criminal business model in the history of malware. With growth numbers cited anywhere from 5-to-8 times more attacks over equivalent periods the year before, ransomware is experiencing an explosion in popularity that regular software vendors can only dream of. While no specific tally of the cost of ransomware in 2016 has been published, the general consensus is that it has easily reached over $1 Billion.

And unlike attacks simply taking advantage of existing known vulnerabilities, ransomware mainly relies on social engineering the end user and is evolving, both technically and as a business. At the time of this report, there were 276 ransomware strains in existence.  And, unlike other malware and cyber attack vectors, we're seeing criminal business models and tactics never seen before.

Ransomware-as-a-Service is now in full swing, where anyone – even those with little technical knowledge – can take advantage of pre-built ransomware complete with a simplified web-based interface and technical support. Competition is so high that criminal groups have hacked and released the decryption keys of competing ransomware vendors! We're now seeing ransomware vendors offering free decryption keys if the initial victim will help infect two other people and have them pay the ransom!

It's pure pandemonium, and, as you'll see, every organization is at risk as the business of ransomware continues to grow.

Nearly every organization is concerned about ransomware, and is doing something about it. The question is what are organizations doing to thwart ransomware, how are they doing it, and if they are successful at stopping it.

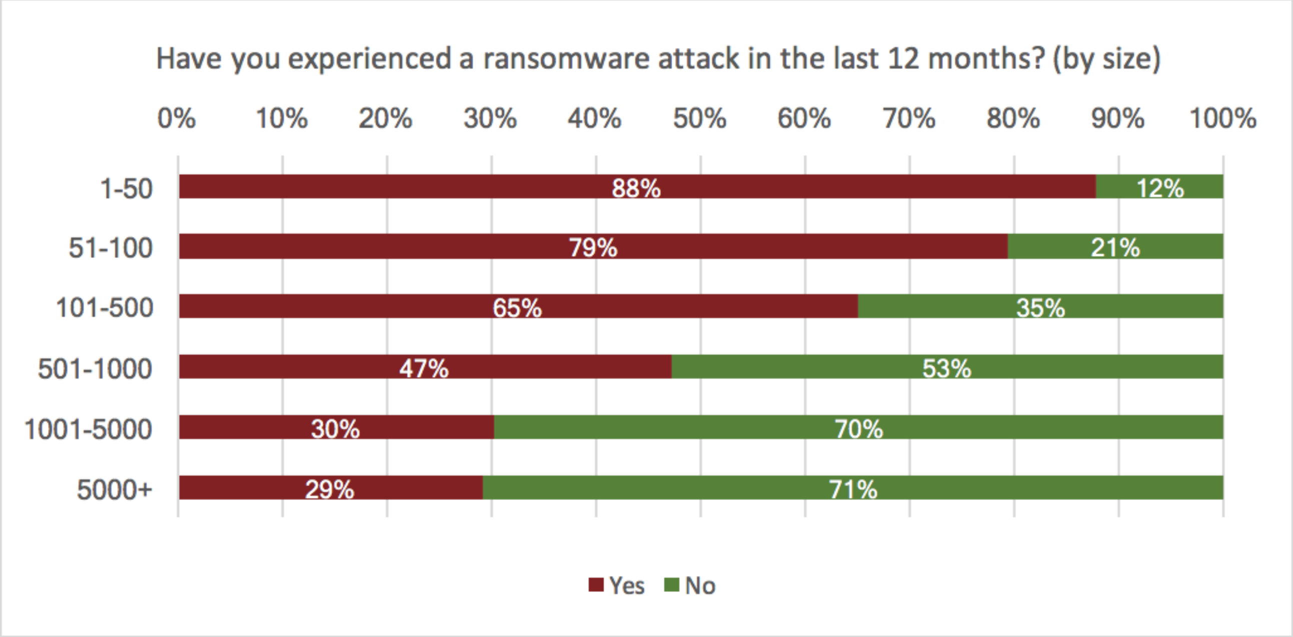
> "While most envision a ransomware attack affecting a single machine, on average we found that approximately 6 endpoints and 2 servers were affected in a given attack. This caused an average of 12 hours of user downtime and 12 hours for IT to remediate the situation."

To find out, KnowBe4 surveyed over 500 organizations about the current state of their ransomware protection, whether they'd been a victim to ransomware, what was the impact, and how did they remediate the attack.

In this report, we'll outline who is at risk, what the scope and cost of an attack is, how organizations are protecting themselves from ransomware, and the effectiveness of those solutions.

## Who's experiencing ransomware attacks?

In a word – everyone. On the average, 33% of businesses have experienced a ransomware attack in the last year. And, it appears as if ransomware is an equal opportunity threat for all industry verticals and sizes of organizations. While every industry represented in our survey was impacted, the technology, healthcare, and manufacturing spaces experienced more attacks than other industry verticals. Ransomware attacks predominantly hit small and midsized businesses (as shown below), although nearly one-third of enterprise organizations (1,000 employees and up) still experienced a ransomware attack in the last 12 months.



## What is the impact of an attack?

Because of the pervasive nature of ransomware, affected machines can be rendered useless through more than just the encryption of data files. Strains of ransomware like Goldeneye encrypt operating system files and the Master File Table (MFT) of the computer. Required data can be made completely inaccessible across the network as well - the CryptoFortress strain, for example, even encrypts data across unmapped network shares. All this adds up to departments possibly sitting on their hands for several days.

“The organizations periodically testing employees saw the lowest percentage (21%) of ransomware attacks in the last 12 months”

## How attacks are being remediated

Realistically, there are only three basic ways to address data and endpoints encrypted by ransomware:

1) Restore the files/endpoint from backups
2) Recreate the lost endpoint/files
3) Pay the ransom for the decryption key

In the early days of ransomware, there was no guarantee that the decryption key would even work. But as ransomware has grown into a worldwide successful business model, it’s far more in the interest of the cyber criminals to have a good, working key, so that the general feeling toward paying the ransom (which is the whole point of this variant of malware) is to pay up.

When either the decryption key doesn’t work, or when the organization has prepared for this day, many organizations opt to simply restore the encrypted data and/or endpoint from backups without paying the ransom.

## Restore the encrypted data

A majority of organizations rely on backups (87%) as their way of recovering encrypted data - this was consistent across both organizations that did and did not pay the ransom. In a small number of cases (a little above 7%) backups were used, but failed. Of those organizations paying the ransom, backups were attempted in all but one case, and were split almost evenly between the backups working and failing.

## Pay the ransom, get the key

According to a recent IBM study, 70% of businesses hit by a ransomware infection pay to regain access to their endpoints and files. However, in our survey, we found the exact opposite; most organizations impacted by ransomware did not pay the ransom (94%). Of those that did pay, the cost was as much as 5 bitcoins (currently worth around $5130), while most paid 3 bitcoins or less. Those organizations paying the ransom were found to be of all sizes.

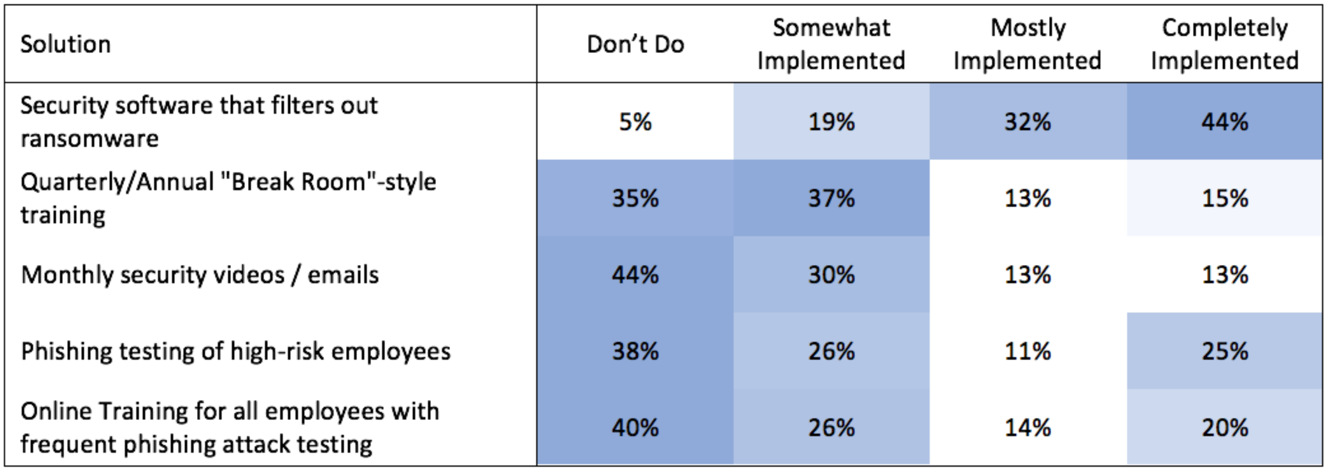
Regardless of which remediation tactic is used, it's an expensive proposition. In either case, it takes a material amount of IT's time to address the ransomware itself (remember, even after obtaining a decryption key, you still need to ensure the ransomware is removed). So, organizations look for ways to prevent ransomware from ever entering into the organization.

## How attacks are being prevented

Every organization puts some measure of defense in place to keep ransomware out. There are a number of tactics used by IT pros today:

- Rely on security-focused software – Fighting evil technology with good technology has been a staple in most IT security strategies. The use of antivirus to test and block links to bad attachments and websites has been around for decades but is less and less effective.
- "Break Room" Training – We've all done it; group everyone in a room once a year and cover the current state of ransomware (among other threats) hoping they'll remember to remain vigilant when it comes time for them to not click that suspicious email link. It's a method filled with good intent, but a lot changes in the world of ransomware within a year's time.
- Monthly Security Training – Usually done via email or using videos, users can educate themselves on topics related to ransomware and other threats – and how to not become a victim. Keep in mind they aren't forced to participate.
- High-Risk Employee Phishing Testing – These infrequent tests focus on employees with access to more sensitive or critical data within the organization. They are subject to a mock phishing attack, with remedial training for those that fail the test.
- Build a "Human Firewall" – Rely on the user to thwart ransomware by first baselining how phish-prone the organization is, having all employees continually participate in on-demand online interactive training to stay current, followed by monthly year-round automated phishing attacks to test all users.

We found (shown below) that the majority of organizations rely on security software, while dabbling in training and testing-related tactics.



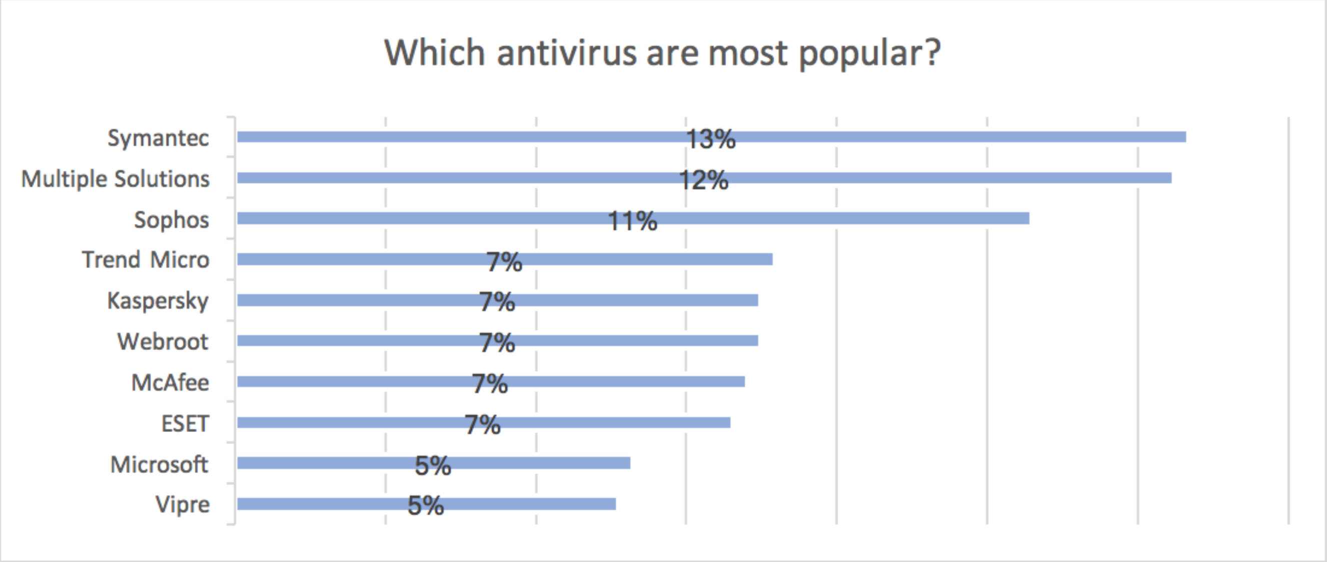
| Solution | Don't Do | Somewhat Implemented | Mostly Implemented | Completely Implemented |
|---|---|---|---|---|
| Security software that filters out ransomware | 5% | 19% | 32% | 44% |
| Quarterly/Annual "Break Room"-style training | 35% | 37% | 13% | 15% |
| Monthly security videos / emails | 44% | 30% | 13% | 13% |
| Phishing testing of high-risk employees | 38% | 26% | 11% | 25% |
| Online Training for all employees with frequent phishing attack testing | 40% | 26% | 14% | 20% |

*Percentage of organizations implementing anti-ransomware solutions*

It's not surprising that most are focused on security software, such as antivirus, to take on ransomware – as antivirus solutions make it their business to stop ransomware, just like every other type of malware. But, is antivirus alone enough?

## The 10 most popular antivirus

Every respondent in our survey indicated they had some form of protection against malware and ransomware. While we asked specifically about which antivirus solution they had implemented, answers ranged from freeware tools to mainstream antivirus solutions, endpoint protection to the use of multiple solutions as a layered defense. With over 40 solutions represented, we limited our focus to the top 10 solutions (listed below).



Not surprising, you can see the more popular antivirus vendors represented, with the 2nd most popular answer being a culmination of many variants of, in essence, "we use tools X, Y, and Z" as their answer.

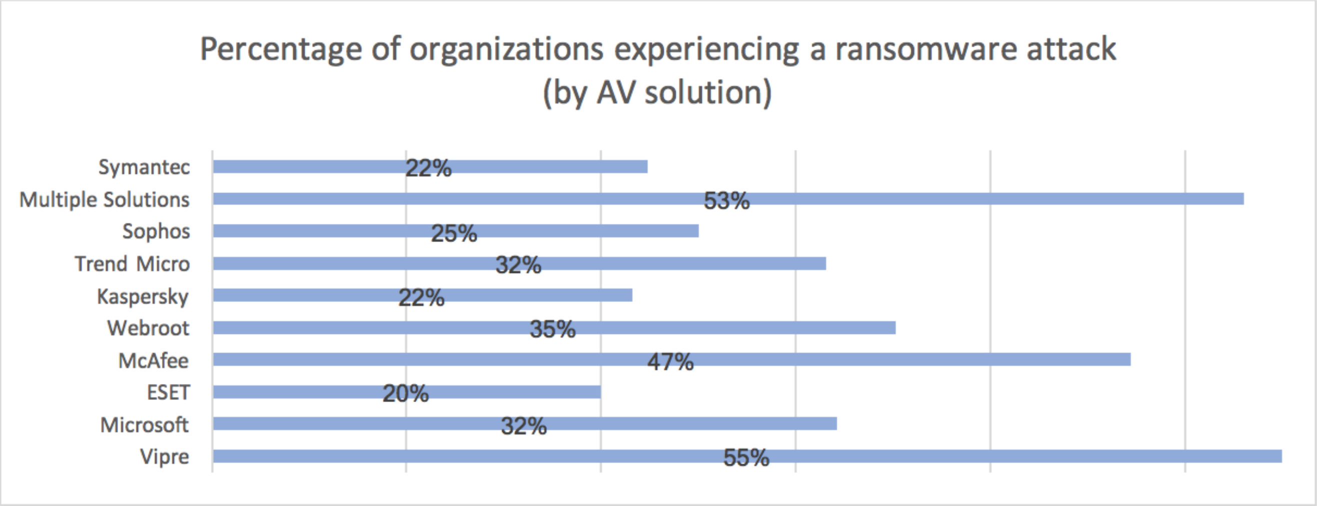
## How effective is antivirus in the fight against ransomware?

Recalling the 33% average percentage of organizations experiencing a ransomware attack, and that every organization has some type of protection in place, it's evident that the solutions in place aren't 100% effective. Surely, it's just the lesser known solutions, right?

**Wrong.**

We found that when looking at the percentage of organizations experiencing ransomware infections based on the antivirus solution they use, every solution still had a material inability to detect and stop ransomware (see below).

The bottom line is even with antivirus, ransomware is going to get in.

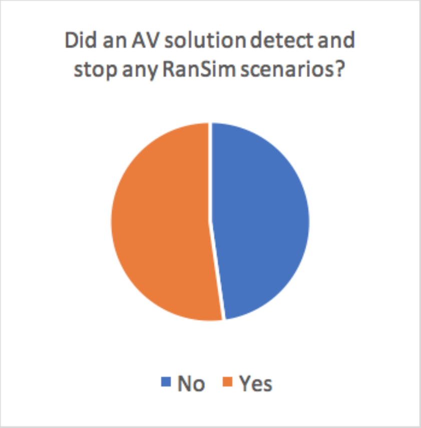


Most surprising was the massive 53% of organizations with multiple solutions against ransomware still becoming victims, despite having a layered defense in place. Whether using one or multiple solutions, there's still some unbelief that these types of solutions simply aren't protecting organizations today. Perhaps it was one really nasty variant of ransomware that got passed all the solutions, right? While we didn't ask about what variant of ransomware hit our respondents, we did double-check their antivirus' abilities using a ransomware simulation.

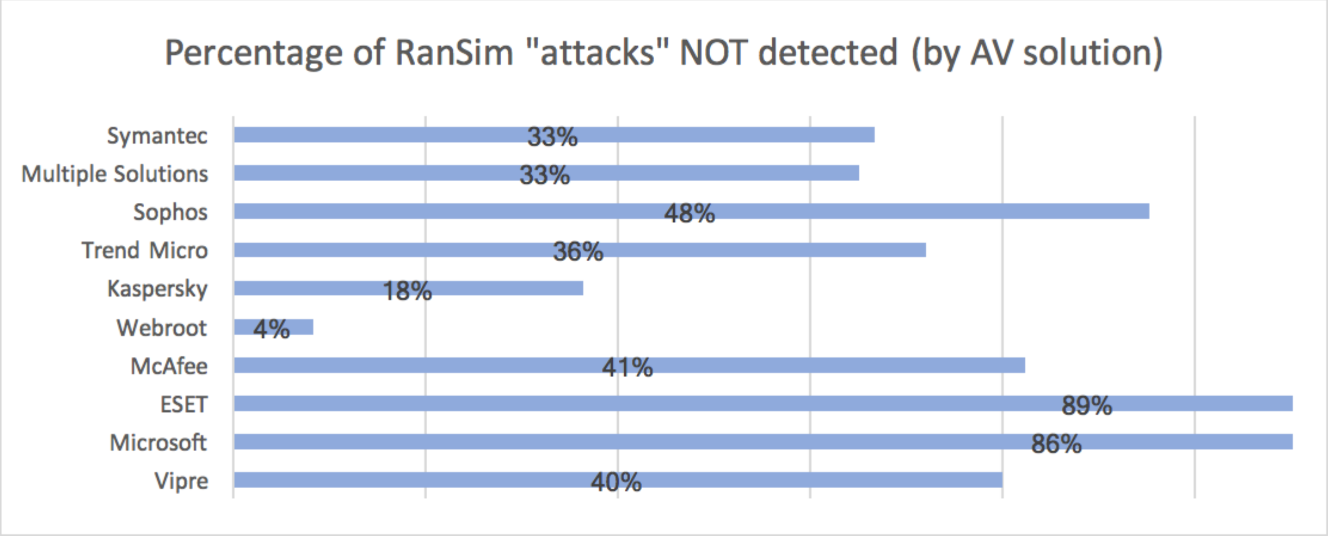
## How about protection against a simulation?

72% of survey respondents had also downloaded KnowBe4's ransomware simulator, RanSim, to test the ability of their antivirus to detect and stop RanSim "attacks". Mimicking 10 different infection scenarios, RanSim attempts to encrypt simulation files it downloads from the Internet, rather than files from the actual endpoint. It functions in the same way that true ransomware does, which should trigger detection by an antivirus solution, and should stop RanSim from running.

Of those respondents who used RanSim, only about half (52%) of organizations current antivirus solutions were able to detect RanSim's ransomware behavior, further demonstrating an inability for existing antivirus solutions to be the sole protection against ransomware.



Most solutions did far worse detecting RanSim than against real-world ransomware, while only one vendor's solution performed materially better (see below).



## Why so ineffective?

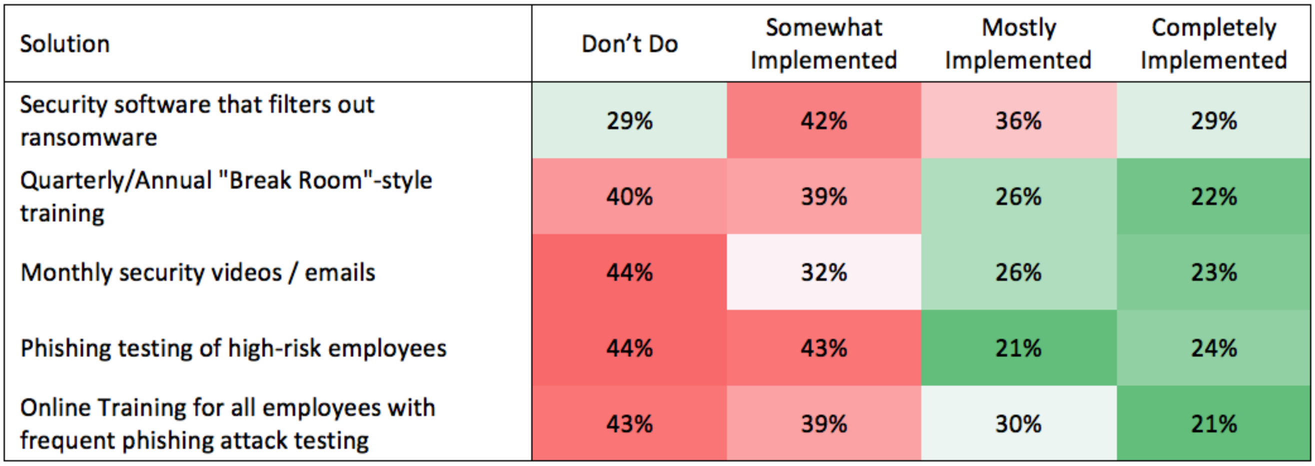
You might wonder why antivirus is so ineffective against ransomware. The answer lies in looking at the threat itself. Ransomware usually utilizes phishing as it's delivery mechanism. Phishing normally uses some level of social engineering – anything from faking an email from the head of HR to simply taking advantage of current events, all in an attempt to manipulate the user to click a link or open an attachment.

Because ransomware relies heavily on social engineering, it becomes critical for organizations to come to the realization that only the user (the one being "engineered") can truly stop all ransomware attacks. Don't click the link or open the attachment, and like magic, don't infect your workstation with ransomware! While antivirus attempts to stop malicious links and attachments, the percent of infection speaks volumes about whether you can truly rely solely on antivirus to protect your organization.

That's why training users combined with simulated phishing attacks have become a part of many organization's anti-ransomware strategy. At the end of the day, the employee is the last line of defense against ransomware and, in many cases, it takes the human mind to recognize that something "just isn't right" about an email.

## Stopping ransomware with security awareness training

We found that having some level of security awareness training in place improved an organization's ability to fend off ransomware. As shown below, those organizations implementing training saw improvement in the percentage of ransomware infections.



| Solution | Don't Do | Somewhat Implemented | Mostly Implemented | Completely Implemented |
|---|---|---|---|---|
| Security software that filters out ransomware | 29% | 42% | 36% | 29% |
| Quarterly/Annual "Break Room"-style training | 40% | 39% | 26% | 22% |
| Monthly security videos / emails | 44% | 32% | 26% | 23% |
| Phishing testing of high-risk employees | 44% | 43% | 21% | 24% |
| Online Training for all employees with frequent phishing attack testing | 43% | 39% | 30% | 21% |

*Percentage of organizations experiencing a ransomware attack (by solution implemented)*

But it's the addition of phishing testing to the training mix that had the greatest impact. The organizations periodically testing employees saw the lowest percentage (21%) of ransomware attacks in the last 12 months. The graph shows that organizations with a well-implemented security culture are much less prone to fall victim to a ransomware infection.

One of the most effective tools to create that security culture is the combination of both training and phishing testing that provided organizations with the greatest ability to stop ransomware attacks. This includes frequent measuring of failure rates of the phishing tests to give the organization feedback on how well it is avoiding being a victim of phishing and if further training is needed.

## Effectively stopping ransomware in 2017

Ransomware continues to evolve in its encryption capabilities, methods of payload delivery, and innovation around inserting itself into an organization. And security vendors work tirelessly to update their technology in this arms race to stop the ever-changing methods of cyber criminals. But even with all the new developments that make ransomware a far more dangerous threat (and the corresponding changes made to security solutions to stop ransomware), the one part of ransomware equation that hasn't changed since the beginning is ransomware's need for an unwitting accomplice.

As this report shows, antivirus solutions help keep some measure of ransomware out, but do little to truly put a stop to ransomware infections. It's only by adding continual testing and training of employees that organizations create their strongest security posture. As cyber criminals continue to invent new ways to bypass security controls, making sure that your last line of defense – the user – is equally up to date is just as, if not more, important.

# Additional Resources

**Ransomware Simulator (RanSim)**
Find out if your endpoint protection actually blocks ransomware infections.

**Free Phishing Security Test**
Find out what percentage of your users are Phish-prone.

**Free Email Exposure Check**
Find out which of your users emails are exposed before the bad guys do.

**Free Domain Spoof Test**
Find out if hackers can spoof an email adress of your own domain.

**Free Phish Alert Button**
Your emloyees now have a safe way to report phishing attacks with one click.

**Ransomware Hostage Rescue Manual**
Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.

**To learn more about our additional resources, please visit www.KnowBe4.com/resources**

## About KnowBe4

KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Thousands of organizations use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilized their end users as a first line of defense.

**For more information, please visit www.KnowBe4.com**

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com