WHITE PAPER | Security Awareness Training

WEBROOT®
Smarter Cybersecurity™

Webroot® Security Awareness Training

The ROI for End User Education

Introduction

While any business that wants to stay afloat must regularly balance monetary costs against benefits, it is especially important for smaller businesses with more limited budgets to thoroughly vet their return on investment (ROI) before purchasing a new product or service. And, depending on budget constraints, many decisions must be made with potential risk in mind. For example, if the likelihood that a business would need a very specific type of costly insurance is extremely low, then there's no point in wasting time or resources on that insurance, right?

But to make an accurate assessment of risk vs. reward, you have to truly understand all the possibilities. Unfortunately, when it comes to cybersecurity, a lot of businesses still don't fully comprehend the risks they face. Perhaps they believe they are too small to make an attractive target for cybercriminals, or perhaps they think their end users would be vigilant enough to recognize and avoid viruses and phishing attacks.

The truth is: any business could be a cybercrime target, no matter its size. In fact, many cybercriminals specifically target small and medium-sized businesses (SMBs), counting on the fact that they are less likely to have adequate security measures.

What's in it for Cybercriminals?

Ultimately, every business holds data that has some worth to cybercriminals on its endpoints and servers. Let's consider the example of a small dentistry office. You might think a dental practice would have little of value to the average cyber-thief, but nothing could be further from the truth. Dentists typically keep thousands of patient records, which include billing information, addresses, phone numbers, and even credit card details. Plus, a dentist's credit card processing system could also become compromised. In reality, healthcare practices are particularly tempting targets for a malicious actor.

Now, let's consider what happens to small businesses in the wake of a cyberattack. It's not just healthcare that has to answer to regulatory bodies (HIPAA, in this scenario) when their customers' data gets exposed. Numerous other industries, such as finance, retail, insurance, energy, utilities, and many more, are subject to compliance regulations. And considering the hefty fines associated with a breach in a regulated industry, not to mention the loss of customer trust, a single cyberattack could easily put an SMB out of business.

Cybercriminals are Intentionally Targeting End Users

End users are on the front lines of a business' defenses. But up to 90% of all successful network breaches[1] are caused by some form of user error. Even if you have a truly robust and comprehensive cybersecurity strategy in place, one wrong click by an unwitting end user could open the door for an attacker. And, according to Microsoft, as security software gets more advanced, it is becoming more expensive for cybercriminals to successfully breach systems. By contrast, it is significantly easier and less costly to trick a user[2] into clicking a malicious link or opening a phishing email.

Phishing scams aren't just cost-effective for criminals, they're also wildly successful. In fact, based on Webroot research from late 2017 in which end users were tested with phishing simulations, roughly 42% of users who opened a simulated phishing email clicked through to the simulated phishing web page, and 65% of people who clicked through[3] tried to enter their credentials. Moreover, 15% of users who fall for a phishing attack once[1] will take the bait a second time.

To see just how prolific phishing attacks really are, we need only look at the data. In the first half of 2017, Webroot saw nearly 1.4 million new phishing sites[4] created each month. Additionally, analyst group ESG conducted a survey in which 63% of organizations surveyed[5] reported having suffered at least one phishing attack in the last two years, while Microsoft reports that phishing constituted 53% of top attacks[2] detected by Microsoft® Office 365® ATP in the second half of 2017 (Figure 1.)

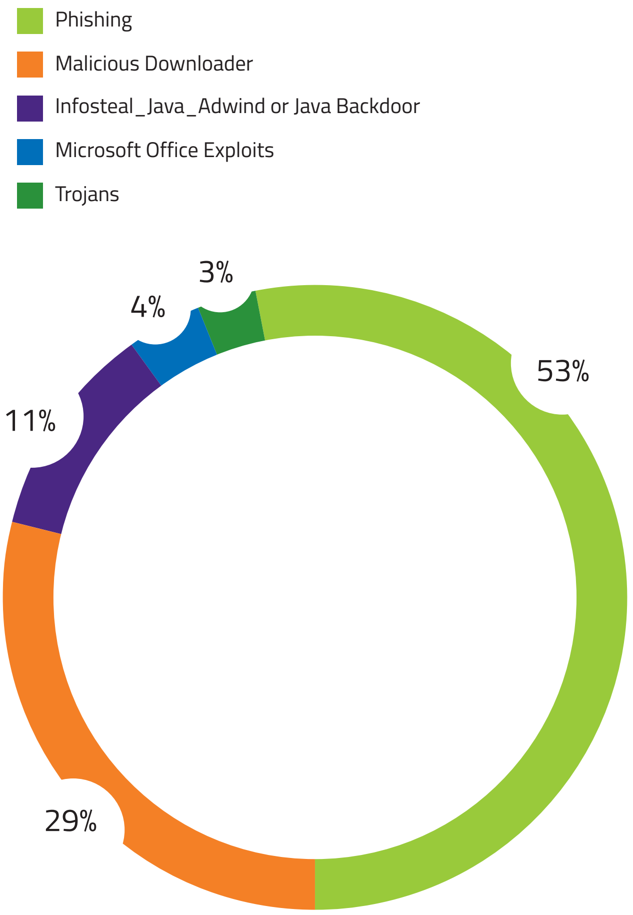

Figure 1: Top attacks detected by Microsoft Office 365 ATP between June and Dec of 2017

Phishing isn't just used to steal credentials. A full 66% of all malware[1] is installed via malicious email attachments. Phishing emails are also responsible for up to 73% of ransomware[6] infections. Faced with such risks, the way forward is clear. Businesses of all sizes and in all industries need to educate end users about cyberattacks and how to avoid them. But that also means they need to allocate enough resources and budget to protect themselves, their employees, their businesses, and their customers' data through cybersecurity awareness training.

Calculating Risk and ROI

Most smaller businesses have begun to agree that their top three most important cybersecurity measures[7] are antivirus or endpoint security, a firewall, and employee education training. But, while the need for cybersecurity spending is clear, it can be difficult to determine which solutions to select. The majority of small businesses cannot afford to make mistakes when committing to potentially expensive security investments, so they must be as effective as possible in their allocation of funds. That's where ROI analysis comes in.

To help you determine the ROI of end user education, we've gathered numbers from a variety of independent surveys and reports user education and security awareness training.

- Companies that roll out training programs see a 26% to 99% improvement in phishing click rates (the average is 64%)[8]
- The least effective phishing simulation program had a seven-fold return on investment, while the average-performing program resulted in a 37-fold ROI[8]
- Detection and recovery from a breach account for 55% of the total cost (35% and 20%, respectively); containment, investigation, incident management, and response make up the rest[9]
- The average cost of a cyberattack has increased by 62% in the last five years[9]
- 36% of businesses who suffered a cyberattack in the last year lost money; 16% expect to lose more money in the next 12 months[7]
- The average annual loss from a cyberattack was $79,841 USD (the median loss was $2,000 USD, while the highest loss was over $1M
- 55% of the information most targeted by cybercriminals is password or authentication data (33%) or payment data (22%)—see Figure 2

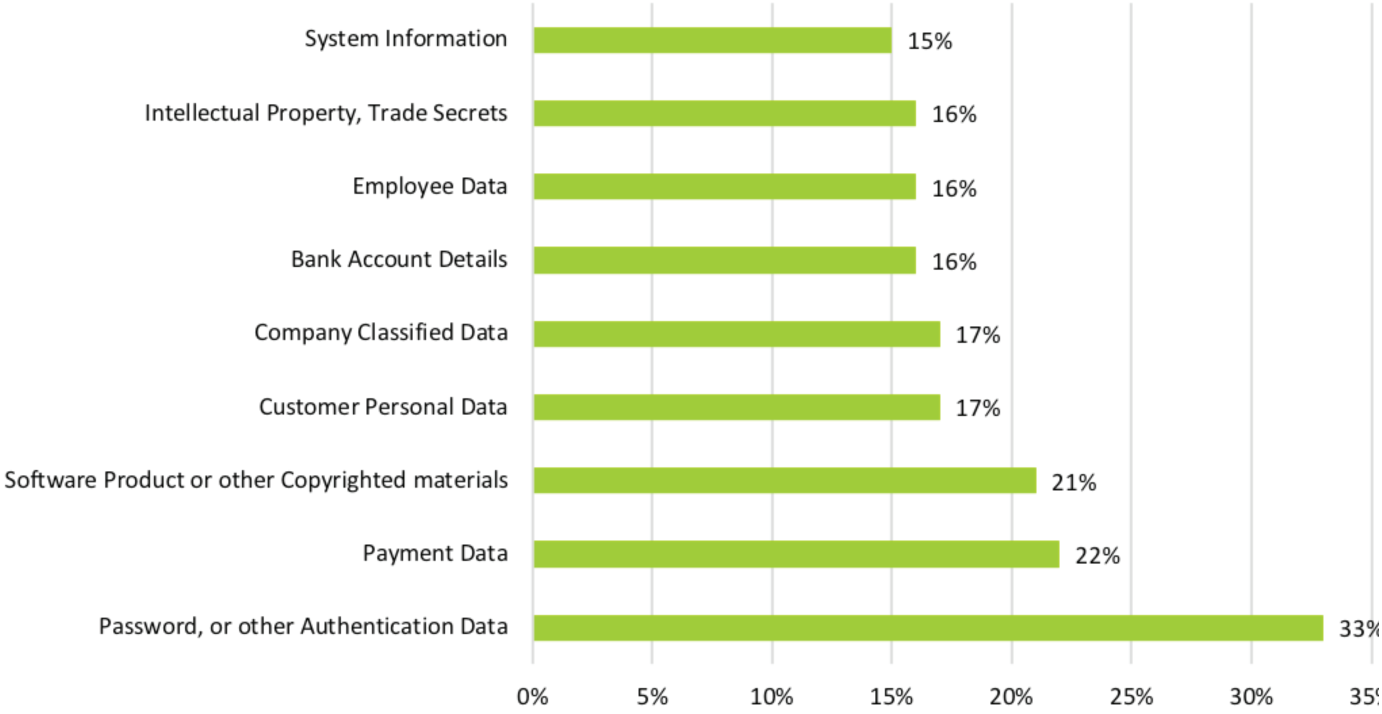

Figure 2. Information most often targeted by cybercriminals

Method 1: Calculating the Return on Security Investment (ROSI)

The Better Business Bureau uses a simplified version of the Gordon-Loeb model[7] for investing in cybersecurity, which offers a useful framework to help businesses find the right solutions for their needs and budgets. BBB recommends the following steps:

1. Estimate Loss

For each information set in your organization—such as emails, a customer database, accounts, employee records, and more—estimate the potential loss that you could incur in a cybersecurity breach, including regulatory fines **($LOSS)**

2. Estimate Risk

For each of the information sets in Step 1, estimate the probability of loss from a cyberattack on that data **(%RISK)**

3. Identify Investments

For each information set in Step 1, identify the potential cybersecurity investments you could make **($INVEST)**

4. Estimate Savings

For each potential investment in Step 3, estimate the reduction in the probability of a breach due to the additional cybersecurity investment **(%SAVE)**

5. Calculate

Compare the investment cost **($INVEST)** to the potential savings where: Potential Savings = **($LOSS) X (%RISK) X (%SAVE)**

As long as the potential savings exceed the cost of investment, then the measure is cost-effective and should be implemented, or, at the very least, strongly considered.

Example

Using the simplified form of the Gordon-Loeb model from the previous section, we have created an example below using figures from third party reports already presented in this document. Our only addition is the retail cost of user education security awareness training for organizations from 10 to 100 employees, which averages to $15 per user per year. The example shows a realistic ROSI case for end user cybersecurity awareness training in a 25-employee business. Keep in mind: while “ROI” or “ROSI” might seem a misnomer, since a cybersecurity strategy does not produce measureable revenue, security products, services, and training provide significant savings by helping prevent costly attacks.

1. Estimate Loss

The average loss from a single cyberattack, per BBB, was $79,841.7 That means the estimated loss is **$79,841 ($LOSS)**.

The actual $Loss relates to the data sets involved in the breach, such as password or other authentication data, payment data, software product, copyrighted materials, customer or personal data, etc. The significance of each depends largely on the business in question and the industry in which they operate. Keep in mind: as we look at the ROSI for user education training, untrained employees are often repeat offenders, so the loss estimate may be on the conservative side.

2. Estimate Risk

The average cyberattack risk for companies in the 10-100 seat range7 is 17%, so the estimated risk is therefore in this example **17% (%RISK)**.

3. Identify Investment

Because our example involves a business with 25 employees, we multiply 25 by a cost of $15 per user per year for end user security awareness training, so the estimated investment is **$375 ($INVEST)**.

4. Estimate Savings

Initial phishing simulation tests typically show that 25-30% of employees click on links or attachments during the first simulation. Following continuous simulations and training, this number drops to the 5% range. So the estimated savings benefit is that the 90% risk from phishing falls from a 1:3 to 1:4 chance (fairly high) to a 1:20 chance (very low). Expressing that reduction in % terms that is a decrease of 80% to 83%! So the estimated saving is **80% (%SAVE)**.

5. Calculate

An investment of **$375** on an average loss of **$79,841** = 79,841 x 17% x 80% = **$10,858**

In this example, the return is **$10,858** on an investment of **$375** so investing on this basis is very cost-effective. Although this return would be reduced slightly when you factor in the time spent by an employee having to complete security awareness training, the cost is negligible.

Method 2: Calculating the Return on Security Investment (ROSI)

The second method we'll cover for calculating the ROSI on security awareness training for end users is based on the risk assessment concepts recommended by CSOonline.com.

- **Single Loss Expectancy (SLE)**
  SLE is the total cost you expect to lose during a single security incident. This can be difficult to calculate because of the differences in value and extent of loss within your information sets. As a guide the minimum number must include the direct costs of the loss, as well as the indirect costs that result from the business impact of that data breach.
- **Annual Rate of Occurrence (ARO)**
  ARO measures the likelihood that a security incident will occur in a given year.
- **Annual Loss Expectancy (ALE)**
  ALE is the total annual financial loss you expect from security incidents. This is a control number, which represents how much money would be lost by taking no additional steps / making no additional security investments. **ALE = ARO * SLE**
- **Modified Annual Loss Expectancy (mALE)**
  Modified ALE uses the ALE above, but also adds in the losses that would be saved by adding and implementing a new security solution. This is calculated by determining the mitigation ratio, which is the percentage of threats deterred by the cybersecurity solution.
- **Return of Security Investment (ROSI) Equation**
  The ROSI equation uses the information above to bring together the risks and associated costs of a security incident, including the impact of deploying a security solution.

$$\text{ROSI} = \frac{\text{ALE * (mitigation ratio – cost of solution)}}{\text{cost of solution}}$$

Example

Using this model with the same base figures and company size as before, we would get the following:

1. Single Loss Expectancy (SLE)

The cost of a successful breach is $79,841, and according to the Ponemon Institute, 20% of indirect costs9 from a breach are due to recovery. In this model we increase the average by 20%, putting the SLE at **$95,809**

2. Annual Rate of Occurrence (ARO)

The likelihood of recurrence in any given year, particularly in the case of phishing attacks, is high. For the sake of this example, we will use a very conservative rate of one breach per year.

3. Annual Loss Expectancy (ALE)

ALE is ARO multiplied by SLE. Here, that would be $95,809 x 1 = **$95,809 ALE**

4. Modified Annual Loss Expectancy (mALE)

This adds in the mitigation rate expected when the business implements security awareness training. In method 1, that was 80%, so **mALE = 80% or 0.8**

5. Return of Security Investment (ROSI)

Using this model we get:

$$\text{ROSI} = 20339\% = \frac{95{,}809 * 0.8 – \$375}{\$375}$$

Conclusion

Although it’s difficult to accurately estimate the true ROI of end user education, the proof is easily established by using phishing simulation test results: educated, cyber-aware users who have undergone training are much less likely to get scammed by phishing, or engage in risky online behaviors. With thorough research and analysis into your level of risk to create realistic variables, these formulas will help you determine which solutions are right for you, as well as how to sell them to the IT decision makers within your own and your Clients’ organizations.

Next Steps

To see how Webroot helps businesses and managed service providers (MSPs) prevent breaches due to human error, visit webroot.com/awareness. You can learn more about how Webroot® Security Awareness Training works and the variety of engaging, interactive course materials we offer, or try it for yourself, free for 30 days.

[1] Verizon. “2017 Data Breach Investigations Report.” (April 2017)
[2] Microsoft. “Microsoft Security Intelligence Report, Vol. 23.” (March 2018)
[3] Webroot Inc. “2018 Webroot Threat Report.” (March 2018)
[4] Webroot Inc. “Quarterly Threat Trends: September 2017.” (September 2017)
[5] ESG. “2017 Business Cybersecurity Trends.” (August 2017)
[6] NTT. “Global Threat Intelligence Report 2017.” (April 2017)
[7] Better Business Bureau. “State of Cybersecurity Among Small Businesses in North America.” (August 2017)
[8] Ponemon Institute. “The Cost of Phishing & Value of Employee Training.” (August 2015)
[9] Ponemon Institute. “The Cost of Cybercrime.” (September 2017)

About Webroot

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George’s Quay Plaza
George’s Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900