LYNX
TECHNOLOGY PARTNERS

KnowBe4
Human error. Conquered.

WHITEPAPER
How to Transform Employee Worst Practices Into Enterprise Best Practices

WHITEPAPER: How to Transform Employee Worst Practices Into Enterprise Best Practices

Preventing your worst data breach nightmare with New School Security Awareness Training

Executive Summary

The press can't get enough of corporate data breaches. They delight in showcasing the latest horror story about a business that lost massive amounts of private records or millions in revenue to the latest hack. You could be next.

Despite all the funds you may have spent on state-of-the-art security software, the bad guys are just one gullible user click away from staging an all-out invasion. To make matters worse, that user might well be you! Recent surveys show that executives can be some of the biggest culprits when it comes to clicking on phishing links and opening malicious email attachments.

Yet by far the most effective strategy in combatting these attacks is also one of the most poorly implemented – security awareness training. The long list of "worst practices" for user education is almost endless – break room briefings while people eat lunch and catch up on email; short instructional videos that provide no more than superficial understanding; and the time-honored practice of hoping for the best and doing nothing.

Find out what the true best practices are for security awareness training – those that establish a human firewall to effectively block hackers and criminals, and keep you out of the headlines.

This whitepaper provides clear direction on how to go about improving your organization's security posture by "inoculating" employees who fall for social engineering attacks. Such incidents are far from uncommon. According to a recent study by Osterman Research, email is the most prevalent channel of infiltration into the enterprise.

> **"The adage is true that the security systems have to win every time, the attacker only has to win once."**
>
> —Dustin Dykes, CISSP
> Founder Wirefall Consulting

Key Points

- A summary of the main email-based attack vectors into organizations such as phishing, spear-phishing, executive "whaling", and "CEO fraud".
- What organizations are doing about it and why this isn't enough.
- What is wrong with most current security awareness training programs. This includes a list of "worst practices" along with why they don't work.
- The proven best practices for security awareness training that reinforce existing defenses by erecting a human firewall.
- How to combine security awareness training with simulated phishing attacks to keep employees on their toes with security top of mind.
- How to devise a valid KPI for the effectiveness of that training to showcase its return on investment.

Understanding the Threat

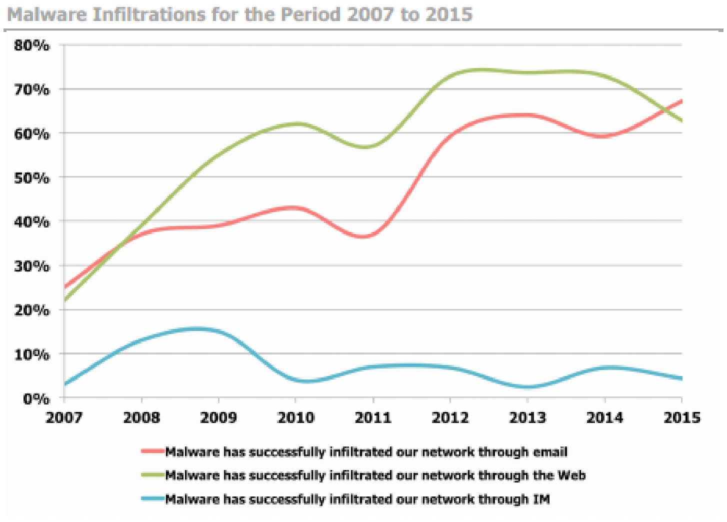
According to a recent study by Osterman Research, email is the top attack vector into organizations. Web-based attacks used to predominate which is why their prevention appears to receive more funding. Yet email attacks were never far away from first place and are now once again in the lead. Osterman places email in the lead with malware infections impacting 67% of organizations, with web-based attacks in second place at 63%.

In third place is a category of attack of uncertain origin. Those attacks may well have come via email but the source has never been detected. 23% of organizations marked this category over the past year, and the true number is probably much higher.

Why can't these companies identify some of the avenues of security compromise? Cybercriminals are becoming more effective. Verizon numbers indicate that 80,000 security incidents were reported by 70 organizations contributing to the survey and over 2,000 breaches occurred in one year.

Here is a summary of the primary email-based attack vectors into organizations:

Phishing: You've all seen examples of phishing emails. They are sent to large numbers of users simultaneously and attempt to "fish" sensitive information from unsuspecting users by posing as reputable sources. This includes banks, credit card providers, delivery firms and law enforcement. Their ploy is to trick the user into either clicking on a link to infect the PC, open an infected attachment or go to a fake website to enter login credentials, financial information, social security data or credit card details. But any data entered is likely to be used maliciously to steal money or an identity, or infiltrate a network. According to the Verizon 2015 Data Breach Investigations Report, 23% of recipients open phishing messages. Another 11% click on attachments. Unfortunately, nearly half open these emails and click on links within an hour of receiving them. Some respond within a minute of receipt. In other words, security teams have a tiny window in which to note the presence of such an attack and take adequate precautions to cleanse it. Clearly, a purely defensive posture is doomed to failure.



Source: Osterman Research, Inc.

Spear-phishing: This malicious strategy takes phishing to a different level. Phishing is spray and pray in that it involves the transmission of one email to a large list, many of whom don't even use that bank, credit card or service. Spear-phishing, on the other hand, is targeted at specific individuals or a small group. The cybercriminal has either studied up on the company or group, or has gleaned data from social media sites in order to gain enough data to con users. The originators craft their messages to make them more believable and increase the likelihood of success. It isn't difficult for the bad guys to find out basic data about employees from the web, Facebook, Twitter, LinkedIn and other similar venues. This can include travel plans, family details, employment history, various affiliations and more. Thus the open rate for spear-phishing is far higher than that of phishing.

Executive Whaling: This practice is becoming increasingly common. The term comes from the Vegas gambling moniker "whale" which means a high roller who is going to lay down some serious money in the casino. After all, the higher up the command chain you go, the more likely you are to find valuable information from your phishing efforts. So cybercriminals are increasingly targeting executive whales. To make matters worse, C-level executives have been found to be some of the biggest culprits when it comes to opening suspicious emails. Perhaps due to their hefty volume of traffic, they don't have the time to look closely before they click. Whatever the reason, whaling is causing some serious breaches inside major corporations.

CEO Fraud: Known variously as the "CEO fraud," or the "business email compromise," highly sophisticated cyber criminals try to social engineer businesses that work with foreign suppliers. This swindle is increasingly common and targets businesses that regularly perform (foreign) wire transfer payments. In January 2015, the FBI warned that cyber thieves stole nearly $215 million from businesses in the previous 14 months through such scams, which start when crooks spoof or hijack the email accounts of business executives or employees. The CEO's email gets spoofed while the CEO is travelling and employees are tasked to transfer large amounts of money out of the country.

"Passive security practices like setting and maintaining defensive security perimeters simply don't work against highly aggressive and adaptable threat sources, including criminal organizations and rogue states."

—Charles King, Analyst
Pund-It

Old School Defenses Are Inadequate

Organizations can't be accused of ignoring the problem. Their budgets reflect that these threats are considered high risk. Money is being spent to upgrade or add new antivirus (AV) software, anti-malware systems, IDS, firewalls, spam filters, security analytics and more. While all of these actions are definitely necessary, they aren't bringing about any marked improvement.

Osterman Research revealed that about half of all organizations feel they made no progress in the past year in combatting phishing efforts and 21% felt they were actually backsliding. This is easy to understand when you consider that the sophistication of malware is growing and the bad guys are far more organized than ever.

Take the case of sandboxing – the practice of placing a potential threat into a system that is isolated from the main network so it can be examined and neutralized. Some malware has appeared that can detect when it has been placed in a sandbox and will remain dormant during that time so as not to alert security personnel of its harmful nature. Other pieces of malware quietly infiltrate a network and are seemingly innocuous. But they are designed to only operate in tandem with other elements. Only when all are present will actual harm result. This strain can be very hard to detect until it is too late.

Verizon notes that phishing is increasingly employed to gain access and then quietly set up camp inside the corporate network. Thus phishing does not always lead to an immediate data breach. Increasingly sophisticated attacks may take their time learning passwords, security defenses and account numbers then stage a sudden attack which transfers millions before being spotted. Alternatively, some hackers have quietly siphoned off small amounts from multiple accounts over many years. Tens of millions disappeared before being detected.

The biggest indictment of traditional security defenses, though, concerns (antivirus) AV software. Still considered the primary defense against malicious programs, the sheer volume of threats is making it impossible for AV to keep up. At the time of this writing, about two million malicious programs are detected every week, according to Virus Total, which provides total malware submissions weekly. It is important to note, though, that AV does not spot all threats. Estimates of AV effectiveness vary from 60 to 98 percent. So at the very least, a few percent of attacks will be missed by AV.

Further, as most AV tools mainly use signature files to detect viruses, new threats are only added to these lists once they are detected. They may have gotten much faster at finding new strains and adding them to their virus signatures – an average of six hours in some cases. But that still leaves a large enough invasion window for the cybercriminals to exploit and cause damage. Time to compromise among Verizon customers was often less than a day once a breach occurred, whereas time to discover the breach was much slower.

Charles King, an analyst at Pund-IT puts it plainly. "It is abundantly clear that traditional security solutions are increasingly ineffectual and that vendors' assurances are often empty promises," says King.

Professional teams of Eastern European cyber mafias exist, for example, that actively hire the best talent in order to innovate new malware strains at a furious pace. This gives them the capability of quickly posting a malicious website, staging an attack on a corporate network and disappearing within a few hours, well before AV companies have had time to update their malware definitions, if the malicious code is spotted at all.

NYSE Governance Services asked top executives just how confident they were that their companies were properly secured against cyberattacks. Only 33% expressed confidence. The same survey found that 81% of executives discussed cybersecurity in most if not all meetings.

This doesn't mean that traditional defenses like AV should be discarded. They all play their part and make it harder for the bad guys to succeed. But they are no longer enough.

What it takes is using any and all of the aforementioned security technologies and strategies as part of a robust and layered defense in depth. But they must be augmented by what Osterman Research considers the "first line of defense in any security infrastructure" – the users themselves. Aberdeen Group called user behavior the "critical last mile" of reducing risks on the prevention side of the security risk equation. In spite of all the technical controls designed to prevent an occurrence, incidents still occur. The root cause for most of these incidents is the action of users. Aberdeen Group concluded that investment in effective security awareness training reduces risk from the financial impact of phishing by 60%.

To some, the concept of a human firewall may appear naive. After all, survey after survey reveals just how gullible users can be. Out of 100 engineering and science majors, for example, one in six fell victim to obvious phishing scams. Another survey showed that 96% of executives failed to tell the difference between a real email and a phishing email.

This is why top executives have become prime targets for whaling attacks. According to research from the SANS Institute, 95% of all attacks on the enterprise network are the result of successful spear-phishing. These attacks no longer only target large companies. They can have dangerous ramifications to any business, regardless of size.

Clearly, modern executives and employees are a ticking time bomb of gullibility ready to explode any organization into the headlines when they fall victim to a clever or even a not-so-clever attack. Steps must be taken to plug this gaping hole. Done correctly, however, these same employees can be molded into an effective human firewall via new school security awareness training. Unfortunately, training efforts of the past have only been marginally effective. Let's take a look at why this is by examining what passes for security training in the ever-evolving world of cyberthreats.

Your Worst Practice Guide to Security Training

It's easy to dismiss security awareness training as unworkable. After all, its results are poor in most organizations. Osterman surveys show that less than a quarter of executives consider it effective. With an IT department continually having to put out fires due to the latest employee or senior executive being tricked into handing over sensitive information, it is understandable that they have little faith in attempts to educate users on phishing and its various schemes.

But the problem is not with the concept of user training itself but rather with the way it is being executed. Here are some of the ways it is traditionally carried out.

Worst Practice #1: Do Nothing and Hope for the Best

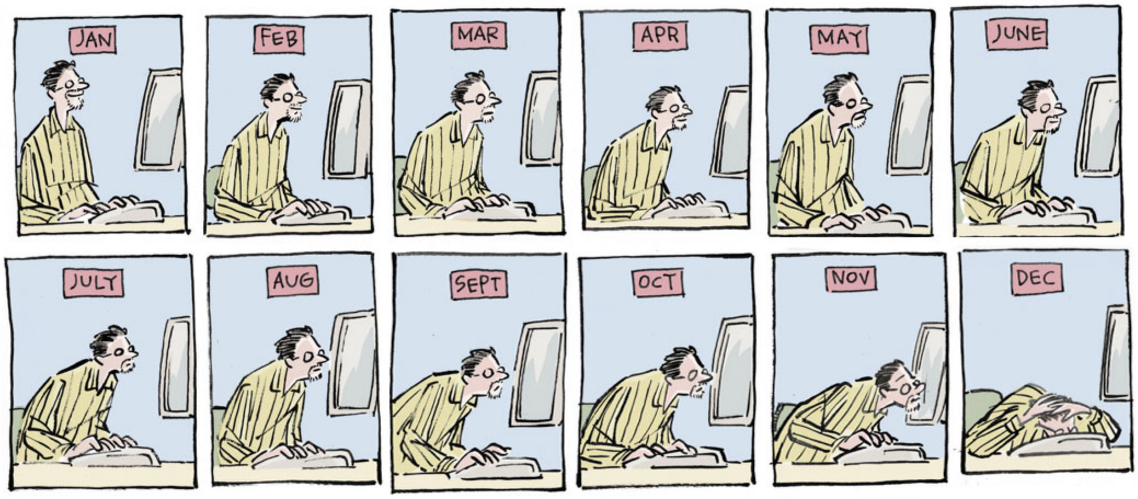
Only about one in five organizations admit to this as their "strategy" against the rise of phishing. But the actual number is probably much higher. The logic goes, "We haven't had a company-threatening data breach to date, and we can live with these minor outbreaks which keep IT busy. So let's hope 'the big one' doesn't happen to us." Aberdeen Group put a hefty price tag on reliance on this strategy. The analyst firm said that there is an 80% likelihood that infections from users will result in total costs of more than $2.5 million per year.

Worst Practice #2: Break Room Training

About 30% of organizations favor the break room approach. They gather as many employees as they can in the break room, provide lunch and have someone from IT or a security expert lecture on topics such as phishing, spear-phishing and whaling. This is certainly better than nothing, but often attendance is low and most of the audience looks upon the event as a time to make some headway on their email backlog. And the results speak for themselves. Measures of the effectiveness of phishing show little change after such briefings.

Worst Practice #3: Monthly Security Videos

This can be done informally with videos made available via email or placed on the website for employees to view, or formally via mandatory classes. These short clips educate users on the perils of promiscuous clicking and on the many snares used by phishers to reel in unsuspecting employees. About one in four organizations gravitate towards this method. At best, this can be categorized as being little more than a superficial training program. On its own, it can't be expected to do much to diminish the risk of data breach. It also causes training fragmentation because important topics are covered months too late.



Worst Practice #4: Phishing Tests

This approach pre-selects high-risk employees only and sends them simulated phishing emails to see how many fall victim to the attack. This is typically paired with some kind of educational module such as links to training modules for offenders as well as short videos to view to increase awareness. The plus on this method is that it offers some kind of metric about phishing. The minus is that employees soon get wise to it and "prairie dogging" begins to happen – an employee sees a phishing test email and pops his or her head up above the cubicle to let the others know to watch out for it. This approach, then, is both limited and too simplistic.

These Worst Practices are the reason why some IT managers struggle to obtain budget approval for more effective security training measures as they struggle to win the fight against phishing. Unaware of the shallowness of their ongoing efforts to proof up staff against attack, executives redline training expenses as "we are already doing that" and buy into vendor hype by throwing money at new technology to deal with latest threat vector. Alternatively, they disapprove security training as the do-nothing approach appears to be working.

Now let's review what the actual best practices are and how to implement them in your organization.

Best Practices for New School Security Awareness Training

The proven best practices for New School Security Awareness Training are designed to add a layer on top of existing firewalls. The goal is to establish an effective human firewall of informed, educated and phish-savvy employees. According to Lance Spitzer, Training Director at the SANS Institute, "One of the most effective ways you can minimize the phishing threat is through awareness and training. You create a network of human sensors that are more effective at detecting phishing than almost any technology."

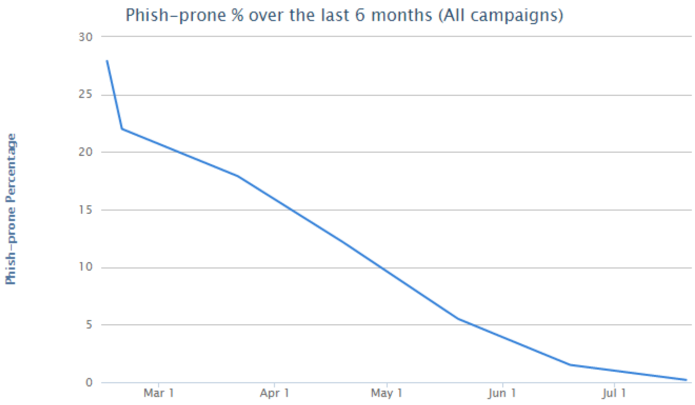
Best Practice #1: Comprehensive Programs Work

Most security awareness programs are superficial at best. They may include some sensible actions, but they don't dovetail into a coordinated and comprehensive program. What is missing is an appreciation of the adversary being faced and the degree of commitment an organization has to have to stave off attacks. It is vital that the C-suite comes to terms with the extent of the threat and the sheer weight of resources the enemy is bringing to bear against naive employees. Only by doing so is it possible for C-level executives to comprehend the measures that must be taken to secure the enterprise and the vital necessity of erecting a human firewall of informed and ever-vigilant users. The crux of this best practice is having an awareness of the scale of the problem and the resources necessary to defend against it.

Best Practice #2: Develop a Coordinated Campaign that Combines Training and Phishing Simulation

Training on its own, typically once a year, isn't enough. Simulated phishing of personnel on its own doesn't work. But together, they can be combined to greatly increase effectiveness. An important best practice is to intelligently integrate these components into an overall campaign. This is best accomplished by finding a platform that integrates simulated phishing and security awareness training.

Best Practice #3: Baseline Phishing Susceptibility



Security awareness training can be undermined due to difficulty in measuring its impact. How exactly are you supposed to prove that it obtains results? All it takes is one fresh outbreak and someone in authority can point to the event as evidence that such training dollars would be better spent elsewhere.

This is where the baseline comes into play. It is vital to establish a baseline on phishing click-through rates so you know the percentage of users who open malicious emails prior to awareness training campaign commencement. This is easily accomplished. Send out a simulated phishing email to a random sample of personnel to find out the number that are tricked into opening an attachment, click on a link or enter sensitive information. This is your baseline phish-prone percentage. This metric can be later used to determine how effective the campaign is. Further, it provides specific numbers that can prove useful during the purchase order approval process.

Best Practice #4: Gain Executive and IT Buy In

To be effective, top executives and IT managers must be onboard. Thus extensive briefings before and during a training program is a must. Briefings are needed in advance to accomplish finance approval, but it should never end there. Prior to beginning a phishing simulation project, communicate to executives and iron out all political or sensitivity issues in advance.

This should include HR, Legal and union representatives where applicable. Otherwise, such campaigns may be unjustly accused of targeting specific employees, undermining morale or discriminating against certain groups. Only by keeping all interested parties involved, listening to their concerns and addressing their needs can the campaign hope to succeed. In some organizations, there may be pressure to inform employees that a simulated phishing campaign is about to be launched. In those cases, where staff are forewarned, the effectiveness of the campaign is significantly reduced.

Another aspect of this best practice is to inform executives about baseline phishing numbers so they are more aware of the extent of the problem and the uphill task facing the organization. Return to this baseline again and again as a means of monitoring results. Showcase all drops in phishing effectiveness as a way to demonstrate the value of the program.

Best Practice #5: Conduct Random-Random Phishing Attacks

Earlier, we mentioned prairie dogging where an employee notices a simulated phishing email and warns the others in the office about it. This phenomenon can even bring about an apparent drop in phishing susceptibility in tests that doesn't translate into the real world. Employees get used to the simulated actions of the campaign, learn to watch out for them every Monday morning and thereafter continue as normal. What you end up with is a simulated phishing initiative that has little or no impact on employee gullibility.

This is particularly important when you consider the findings from a study by Proofpoint. It found that no company had a zero click rate from phishing attacks. While repeat clickers account for the majority of clicks on malicious links, 40% of clicks are typically one-off clickers. In other words, even the best and the brightest can be caught unawares and will click on something malicious from time to time. Prairie dogging might allow these rare but occasional phishing victims to develop complacency.

The way to guard against this is to use what are termed random-random simulated phishing attacks. This New School Security Awareness Training practice entails the selection of random groups, random schedules, and random phishing templates to gain a more accurate estimate of an organization's likelihood to fall victim to phishing. Instead of sending out the same phishing emails every Monday morning to accounting, every Tuesday at lunch to sales and every Friday evening to manufacturing, switch the tactics and schedules around by varying the groups and schedules randomly. This eliminates prairie dogging and provides the organization with a real metric they can use to determine effectiveness.

Best Practice #6 Personalize Emails

Personalized emails are more believable. In some cases, this can be as simple as adding the employee's first name. But in large organizations, personalization must be taken further. For example, obtain from payroll the names of the banks used by employees for direct deposit and use that bank name in a phishing campaign. Another tactic is to split phishing email into groups such as by departments, or to tie phishing emails into topical or popular events.

> **"Verizon notes that phishing is increasingly employed to gain access and then quietly set up camp inside the corporate network."**
>
> —Osterman Research

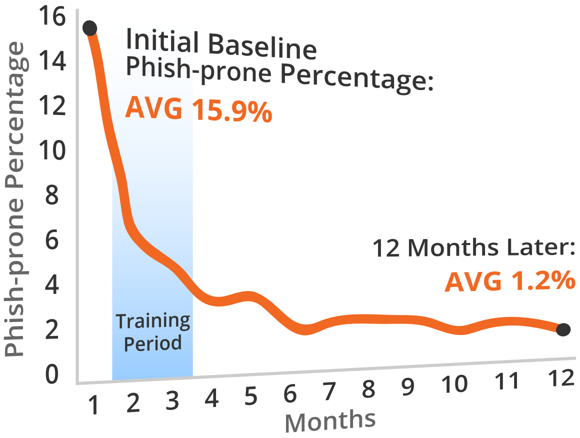
Best Practice #7: Don't Expect Miracles

The results from New School Security Awareness Training are excellent. But they fall short of the miraculous. By that, we mean phishing victimization rates generally fall from the 10-25% range to about 2%. It appears that getting below that point is extremely difficult. But continuation of the campaign can keep results at or below that level, which will have a significant impact on the organization. With malware infections caused by phishing minimized, IT finds itself able to contain remaining outbreaks more effectively as there are far less of them.

Due to the dramatic drop in infections, other security measures have a greater chance of success. IT finds itself moving from constant troubleshooting mode to being able to move forward with projects that provide greater strategic value to the organization.

Best Practice #8: Avoid Witch Hunts

A common concern about simulated phishing is that the results could be used in witch hunts. Therefore, don't ever use results in this way or bring them up in annual reviews. It is best to keep results general and use them to correct and train the organization as a whole as opposed to singling out specific individuals.



The exception to this comes once the coordinated campaign of training and phishing simulation has brought about marked results. After a prolonged series of simulations and training steps, and once the numbers have bottomed out, companies are likely to find the same small group of repeat offenders. Proofpoint noted that less than 10% of users are responsible for almost all clicks on any given wave of malicious attacks. While New School Security Awareness Training can push that number down far lower, there will remain a handful of individuals who continue to click despite being given every opportunity to reform.

By this point, they will have attended several training classes, and received a thorough education on how phishing can fool them. Yet they go on being fooled no matter what remedial steps are taken. Now is the time to involve HR to take up findings with repeat offenders who show no improvement despite several attempts at retraining. To take any possible negative connotation away from 'flunking' simulated phishing tests, it sometimes works to incentivize departments to encourage their staff to complete training or retraining in an effort to achieve a 0% click rate. Those doing so, or scoring below a particular level can be awarded with gift cards or other inducements.

Best Practice #9: Continue to Test Employees Regularly

Even when testing confirms that phishing susceptibility has fallen to nominal levels, continue to test employees frequently to determine if anti-phishing training remains effective. The bad guys are always changing the rules, adjusting their tactics and upgrading their technologies. Therefore, training reinforcement must remain a part of the organizational security arsenal in order to keep pace with constantly evolving threats.

Best Practice #10: Provide Thorough Security Training

Old school security training favored a lecture or video approach. The problem with this type of training is that it can rapidly become outdated – the security landscape of one year ago is very different from that of today. It also focuses too much on theory and isn't balanced by practical application. New School Security Awareness Training is interactive, balances theory and application, is continually updated, and is based upon thorough insight of how cybercriminals operate. Ideally, it will incorporate the services of an expert hacker who knows all the ways of entering an organization and all the tricks of the phishing trade. It should make sure employees understand the mechanisms of spam, phishing, spear-phishing, malware, ransomware and social engineering, and are able to apply this knowledge in their day-to-day jobs.

Conclusion

It is obvious that IT security must be significantly improved on all fronts. Organizations must seek out and adopt the latest methods available in order to keep one step ahead of ever more resourceful organized cybercrime. However, many of the budget dollars spent on such programs will be wasted unless this technology is supported by New School Security Awareness Training programs reinforced by frequent simulated, randomized phishing attacks. The consequences of failing to do so go well beyond bad headlines. The estimated financial loss from 700 million compromised financial records in 2015 was $400 million, according to Verizon. One well-publicized data breach can lead to lost jobs (including that of the CEO, CIO and CISO), rising legal costs, non-compliance penalties, loss of brand reputation, customer churn, and a major hit on the bottom line.

About Lynx Technology Partners

Lynx Technology Partners delivers dynamic Cyber Security and Risk Management solutions for our customers helping them understand and navigate their threat landscape. The Lynx Team is made up of experienced, industry recognized experts who have led governance, risk management, compliance and cybersecurity programs and served as subject matter experts (SMEs) for Fortune 500 enterprises and Federal agencies.Lynx combines risk management professional services with an Integrated Risk Management Platform to better manage risk throughout the people, process and technology lifecycle.

Our dedication to customer success and responsiveness to needs has earned us the trust of a growing list of customers in highly regulated industries worldwide.

For more information, please visit www.LynxTechnologyPartners.com

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 by two of the best known names in cybersecurity, Kevin Mitnick (the World's Most Famous Hacker) and Inc. 500 alum serial security entrepreneur Stu Sjouwerman, to help organizations manage the problem of social engineering tactics through new school security awareness training.

More than 1,700 organizations use KnowBe4's platform to keep employees on their toes with security top of mind. KnowBe4 is used across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance.

LYNX TECHNOLOGY PARTNERS

KnowBe4
Human error. Conquered.

Lynx Technology Partners | InsideSales@LynxTP.com | 1 (800) 314-0455