KnowBe4
Human error. Conquered.

REPORT

Security Awareness Training Deployments Deter, Defeat Hackers

REPORT: Security Awareness Training Deployments Deter, Defeat Hackers

Executive Summary

"KnowBe4's training has empowered our employees to be vigilant and less susceptible to legit fraudulent and malicious emails, which we definitely have encountered... Any organization that doesn't think they need IT security training is fooling themselves. This is based on our experience with the number of failures we initially had on the phishing tests, and the progress we've made over the last couple years. We reduced those failures to almost none. No one wants to be in the dreaded "Clickers" group, lol. Trust me!" IT Director at an SMB Manufacturing firm in Illinois.

Nearly two-thirds of corporations – 64% – say security awareness training helps their businesses to identify and thwart hacks immediately upon deployment. And, an 86% majority of corporations say security awareness training (SAT) decreased overall security risks and educated employees to the ever-present danger posed by cyber security scams.

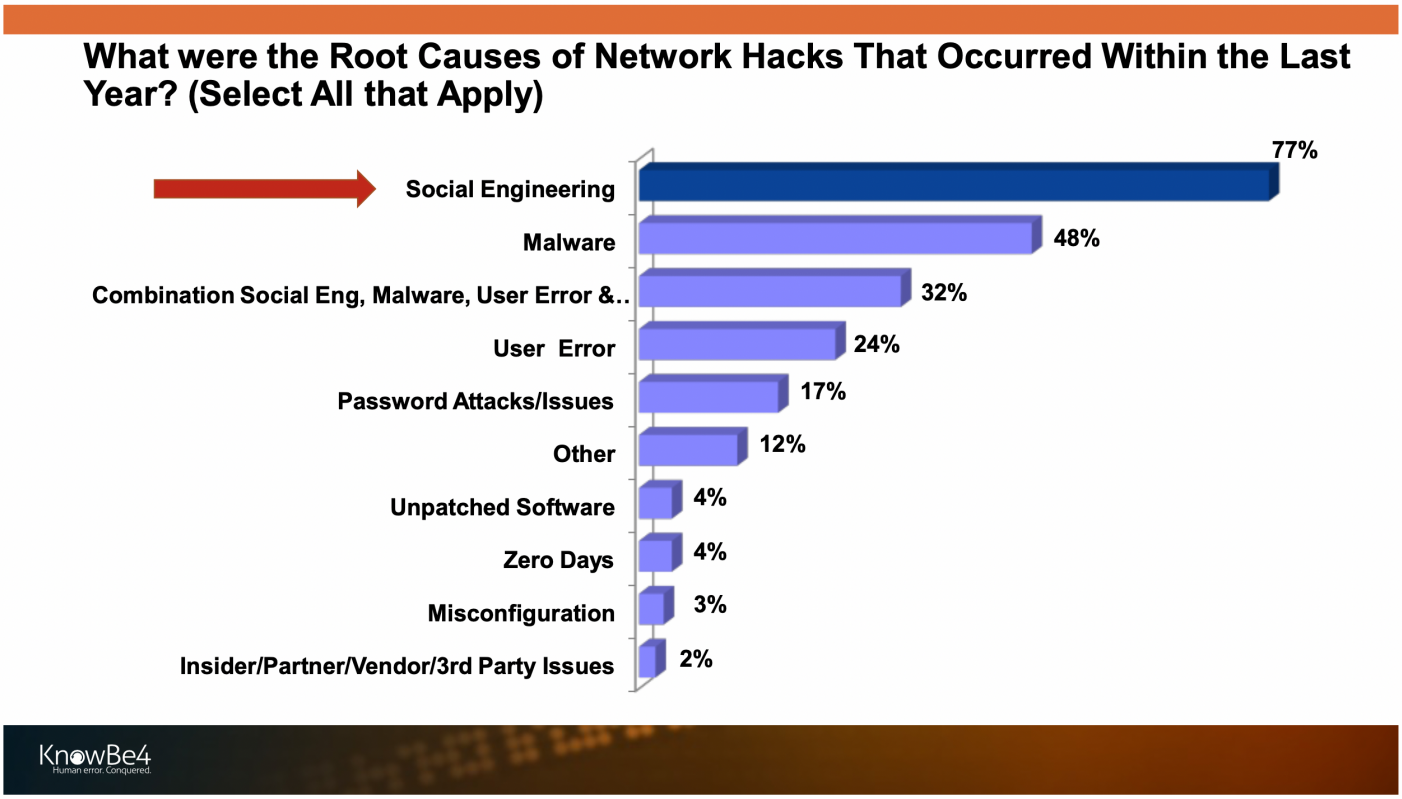
Those are the findings of the KnowBe4 2018 Security Awareness Training Deployment and Trends Survey. This annual, independent web-based survey polled 1,100 organizations worldwide during August and September 2018. The study queried organizations on the leading security threats and challenges facing their firms as cyber security attacks increase and intensify.

The study also polled organizations on the initiatives they're taking to proactively combat the growing diversified and targeted cyber threats. The study found that 88% of respondents currently deploy (SAT) tools. The businesses report that the training plays a pivotal role in identifying and thwarting attacks; minimizing risk and positively changing the employee culture.

Among the other top survey findings:

- Social engineering was the top cause of attacks, cited by 77% of respondents, followed by malware (44%); user error (27%); and a combination of the above (19%); and password attacks (17%). (See Exhibit 1).
- Some 84% of respondents said their businesses could quantify the decrease in successful social engineering attacks (e.g., phishing scams, malware, zero day, etc.) after deploying SAT to their end users after just a few simulated exercises. This is based on 700 anecdotal responses obtained from the essay comments and first-person interviews.
- On average, respondents reported that Social Engineering cyber hacks like Phishing scams and Malware declined significantly from a success rate of 40% to 50% to zero to five percent after participating in several KnowBe4 SAT sessions.
- Almost three-quarters – 71% of survey participants – indicate their businesses proactively conduct simulated phishing attacks on a monthly, quarterly or weekly basis.
- An overwhelming 96% of respondents affirmed that deploying SAT and simulated phishing changed their firm's computer security culture for the better, making everyone from C-level executives to knowledge workers more cognizant of cyber threats.

Exhibit 1. **A 77% Majority of Firms Cite Social Engineering as Top Cause of Security Breaches**



Source: KnowBe4 October 2018

This report details the real world cyber threats facing organizations using empirical survey data and customer interviews. The survey results illustrate and emphasize the necessity of deploying security awareness training and simulated phishing to secure valuable data assets, educate end users and minimize risk.

Introduction

In the 21st century, organizations can no longer practice security with 20/20 hindsight.

Complacency and ignorance regarding the security of the organization's data assets will almost certainly lead to disaster. Not a day goes by without a major new cyber hack reported.

Threats are everywhere. And no organization is immune.

Hackers are sophisticated, bold and hone in on specific targets. The hacks themselves are more prolific, pervasive and pernicious.

The current computing landscape includes virtualization, private, public and hybrid cloud computing, machine learning and the Internet of Things (IoT). These technologies are designed to facilitate faster, more efficient communication and better economies of scale by interconnecting machines, devices, applications and people.

The downside: increasing interconnectivity among devices, applications and people produces a "target rich environment." Simply, there are many more vulnerabilities and potential entry points into the corporate network. IT and security administrators have many more things to manage and they can't possibly have eyes on everything. Oftentimes, the organization's end users pose the

biggest security threat by unknowingly clicking on bad links. But even "trusted" sources like supposedly secure third-party service providers, business partners or even internal organization executives can unwittingly be the weak links that enable surreptitious entry into the corporate network.

The ubiquitous nature and myriad types of threats, further heightens security risks and significantly raises the danger that every organization – irrespective of size or vertical market – will be a target. The accelerated pace of new cybersecurity heists via social engineering, (e.g., phishing scams, malware, password attacks, zero day, etc.), makes the IT security administrator's job extremely daunting.

Consider the following:

- The Verizon 2018 Data Breach Investigations Report revealed that within the last 12 months, there were over 53,000 incidents and 2,216 confirmed data breaches.
- The AT&T 2017 Global State of Cybersecurity, Mind the Gap: Cybersecurity's Big Disconnect found that 65% of firms said their in-house cybersecurity capabilities adequately protect against cyber threats. However, 80% of organizations say they've suffered a breach within the past year.
- The website Hackmageddon, which publishes bi-weekly statistics on cybersecurity, found that there were a total of 950 major cyber attacks in 2017 and the main motivation behind them was cyber crime in 77% of the occurrences.
- RevisionLegal an Internet law firm specializing in securing intellectual property rights said it identified 658 cybersecurity breaches from January through June 2018
- In July 9, 2018 article, "The Worst Cybersecurity Breaches of 2018 So Far," Wired Magazine reported that during the first six months of 2018, there haven't been as many government leaks and global ransomware attacks as there were by this time last year." However, the article went on to state that "corporate security isn't getting better fast enough, critical infrastructure security hangs in the balance, and state-backed hackers from around the world are getting bolder and more sophisticated."

Security issues and vulnerabilities are not new.

Organizations have long grappled with the dilemma of implementing strong security versus the monetary cost, training and usability issues associated with maintaining a strong security infrastructure. This is true for small organizations with two to 25 employees, to the largest global multinational enterprises with hundreds of thousands of workers.

A security breach that damages or destroys data and interrupts a large enterprise's network operations for even a few minutes can result in losses of millions per minute depending on the type of security breach, the duration, severity and the timing of the event (e.g., occurrence during peak usage hours or during a major business transaction).

System and network security are just as crucial if not more so, to small businesses. In most cases SMBs lack the financial and technical resources of their large enterprise counterparts. They are more financially vulnerable to the impact of moderate and prolonged outages and typically not able to pay for extensive legal fees.

Remediation efforts to discover and fix the source of the vulnerability, assess the extent of the damage and perform "make good efforts" with any customers, business partners or suppliers that were impacted by the security breach, are time consuming and costly for all organizations. The rapid pace of technology advances, coupled with the adoption of technologies like the

Internet of Things (IoT), machine learning, analytics, virtualization and cloud computing and Bring Your Own Device (BYOD), remote access and mobility make it even more challenging for organizations to stay abreast of the numerous internal and external threats and safeguard their systems and networks. Organizations that fail to implement the appropriate security mechanisms and obtain the necessary security training increase their risk, raising the possibility of greater collateral and legal damage in the event of a successful security penetration.

Fortunately, there is help in the form of security awareness training and simulated phishing which immediately assists organizations in educating employees from the boardroom to the mailroom transforming the corporate culture from one that is lax to one that is alert and vigilant.

Data and Analysis

Computer and network security has all too often been practiced with 20/20 hindsight. That is, organizations have been lax in implementing and enforcing strong computer security policies. And have been remiss in deploying adequate security mechanisms to safeguard corporate data assets and intellectual property – unless or until, the company suffered a significant data breach.

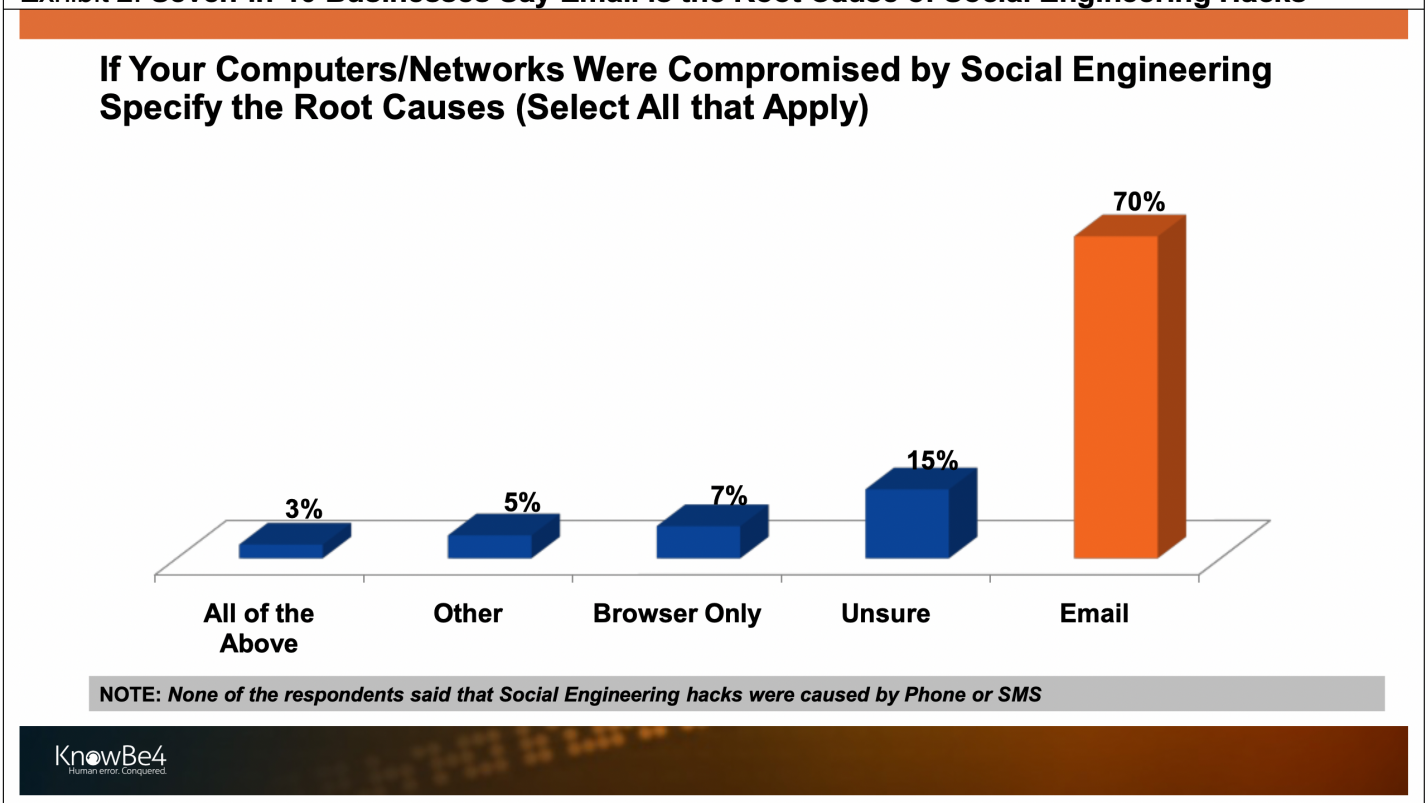
The KnowBe4 2018 Security Awareness Training Deployment and Trends Survey results indicate a majority of organizations recognize the increasing danger posed by myriad pervasive and pernicious cyber threats. Organizations are also acutely aware that security and IT managers and administrators cannot possibly have eyes on everything, as the size, scope and complexity of their respective infrastructure increases along with the number of interconnected people, devices, applications and systems. Hence, companies are now proactively assuming responsibility for safeguarding their data.

New-school SAT and simulated phishing is a cost effective and expeditious mechanism for heightening user awareness of the multiple security threats facing organizations.

Among the other survey highlights:

- Among businesses victimized by social engineering, some 70% of respondents cited email as the root cause (See Exhibit 2). This is mainly due to end users clicking without thinking and falling prey to a wide range of scams such as phishing, malware and zero day hacks. Another 15% of respondents said they were “unsure” which is extremely concerning.
- An 88% majority of respondents currently employ security awareness training programs and six percent plan to deploy one within six months.
- An 86% majority of security awareness training Programs conduct simulated phishing attacks and that same percentage – 86% – firms randomize their simulated phishing attacks.
- Some 71% of respondents that deploy KnowBe4’s security awareness training said their firms had not been hacked in the last 12 months vs. 29% that said their companies were successfully penetrated (even for a short while before being detected and removed).
- Survey respondents apply security awareness training programs in a comprehensive manner to ensure the best possible outcomes. Asked to select all the mechanisms they use in their SAT programs: 74% said they use email; 71% employ videos, 43% of organizations said they use human trainers; 36% send out newsletters and 27% engage in seminars/webinars with third parties.

Exhibit 2. **Seven-in-10 Businesses Say Email is the Root Cause of Social Engineering Hacks**



Source: ITIC/KnowBe4 November 2013

KnowBe4's security awareness training study revealed that complexity and a lack of training for IT professionals and end users alike, exacerbates the already difficult task of securing servers, desktop devices (PCs, notebooks/laptops, tablets and smart phones) and the overall network.

In the absence of any significant security vulnerabilities, it's easy for companies to be lulled into a false sense of complacency. This can present a conundrum for IT departments when they attempt to convince C-level executives to allocate capital expenditure funds for security products and training at a time when budgets are still tight.

Social Engineering and Phishing Scams

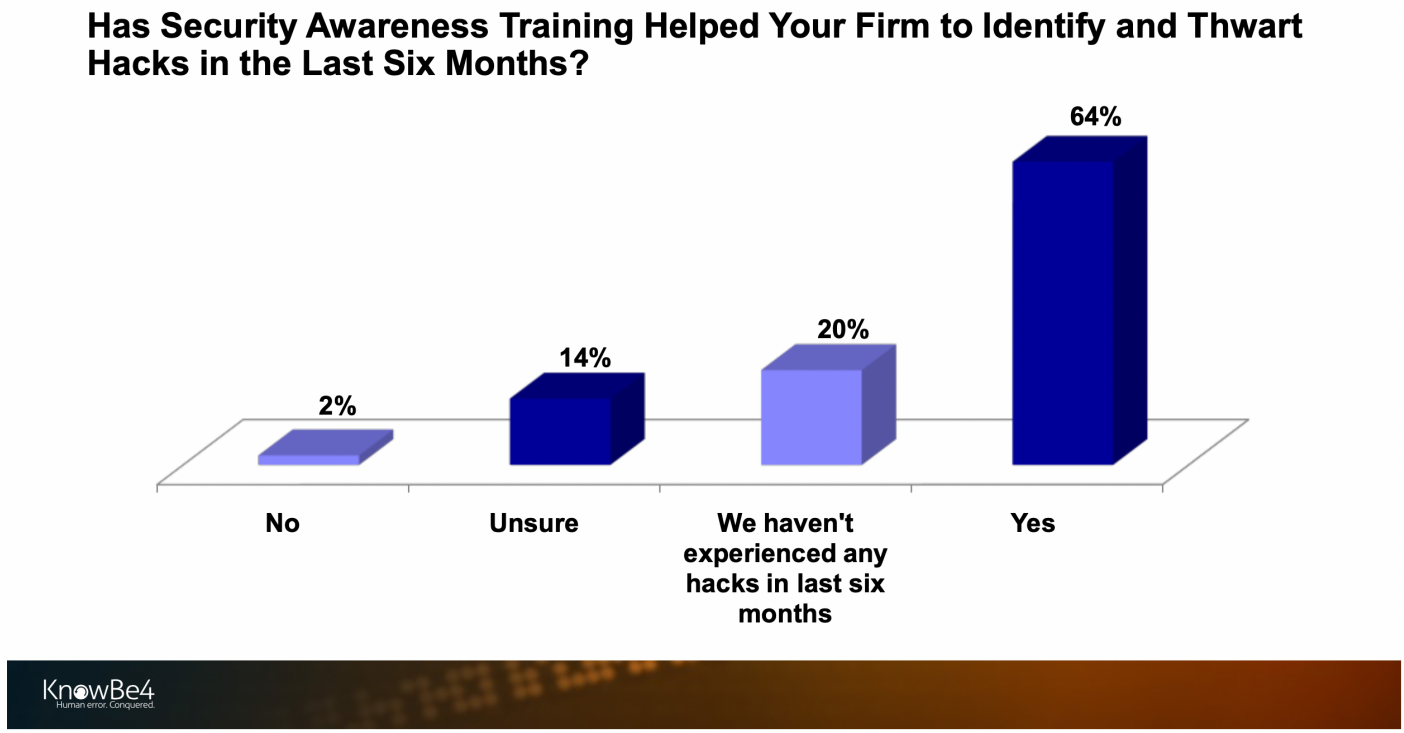
To reiterate, the survey data found that currently social engineering (e.g., phishing scams with email as the root cause) and malware currently constitute the biggest security risk. As such, businesses are focusing much of their attention on repelling these attacks by stepping up their security awareness training initiatives.

- Overall, 71% of organizations now proactively schedule simulated phishing attacks on a regular basis. Nearly four in 10 companies – 38% – conduct simulated phishing attacks monthly; 21% quarterly; 12% weekly; 9% ad hoc and 6% as needed.
- Some 40% of firms that conduct simulated phishing attacks focus on specific groups with specific types of phishing (e.g., CEO fraud) vs. 38% that do not.
- And 53% of respondents automate their simulated phishing attacks to send SAT components to anyone who fails the test. Another 21% of corporations polled said they plan to do so in the future vs. 26% that do not.
- The amount of time administrators spend managing SAT programs annually – varies widely. One-third – 33% – say as needed and 27% say no specific amount of time.

- The amount of time corporations require their employees to spend taking security awareness training also exhibited a wide degree of variance. About 30% said no specific time allotted; 22% indicated 31 to 60 minutes and 17% said one to two hours.

Security awareness training yields positive outcomes and delivers near immediate Return on Investment (ROI). As Exhibit 3 illustrates, nearly two-thirds or 64% of survey respondents indicated that the training helped their companies to identify and thwart security hacks within the last six months – either by alerting them to a potential vulnerability or attempted hack and allowing them to block the threat – or by enabling security and IT administrators and users to recognize rogue code and quickly remove it before it could cause damage. Another 20% of those polled claimed their firms had not experienced any hacks in the last six months.

Exhibit 3. **Over Six-in-10 Businesses Say Security Awareness Training Thwarts Security Attacks**



Source: ITIC/KnowBe4 October 2018

Most notably, as Exhibit 3 shows, only a small two percent minority of respondent companies said security awareness training did not help their firms to avert attacks. KnowBe4 delved more deeply into the responses of the two percent of customers who said SAT programs had not helped their organizations to avoid a security breach and found that the organizations didn't fault the training solutions.

Rather, the survey respondents said the fault lay with upper management for not advocating more strongly for SAT usage within their firms. Another group of customers noted that their corporate security was compromised by a trusted third-party provider who was hacked, or that the successful phishing attack was the result of hackers who targeted a specific – usually high-ranking company executive – with an extremely sophisticated hack.

However, even in those instances where respondents said their firms had been victimized, they also acknowledged the positive outcomes the corporation realized by installing SAT packages and

running the simulated attack drills.

"I would say it has helped extremely, however, because it is not enforced or mandated many of our sales people have not watched the videos and completed the awareness training. This allowed a few "hacks" through emails that were disguised as Microsoft Office User ID and password re-entry needs. This allowed the "hacker" to redirect these emails to a Gmail and then send out spam to many other users and clients." operations coordinator at an SMB insurance firm in California

"My biggest takeaway from doing our security awareness program for the past year is that if it is not made mandatory for everyone by upper management, people will not complete the training. Our participation rate for the program is 50%, and most of the people not participating are the ones not required to do so by their managers. These people are also more likely to fail our phishing simulations, and they often exhibit other risky behaviors such as logging in as administrators and surfing the web, checking email, etc. It is definitely a challenge to get our senior managers to understand the importance of making security training mandatory for everyone." security administrator at a midsized utilities company in Colorado

"Security awareness training has not only helped make our company safer, but has also made our employees' families safer. The knowledge we share with our employees can and does translate to their family's online/offline safety. Working together, we can be stronger against the ever-growing threat that we are posed with daily." VP of IT at a midsized transportation company in Illinois

"...End users, employees and contractors are the weakest link in your systems. You can patch systems to protect them from the newest vulnerabilities, but security awareness training is the closest thing to patching your end users. I've done short comments at group meetings on security, but I've found that showing managers and end users phishing test results, they understand that if it was real, they'd have failed really opens their eyes. The most important piece is getting buy-in from managers and employees that they are an important piece. If they assume that the IT department keeps them safe and blindly trust everything sent their way, it's only a matter of time before a breach occurs. I believe it also helps them understand the need for pain points such as 2FA and other safeguards by making them part of the solution." IT administrator at a transportation SMB in Connecticut

An architect at large government agency in Albany, NY said his organization implemented security awareness training after two significant security breaches.

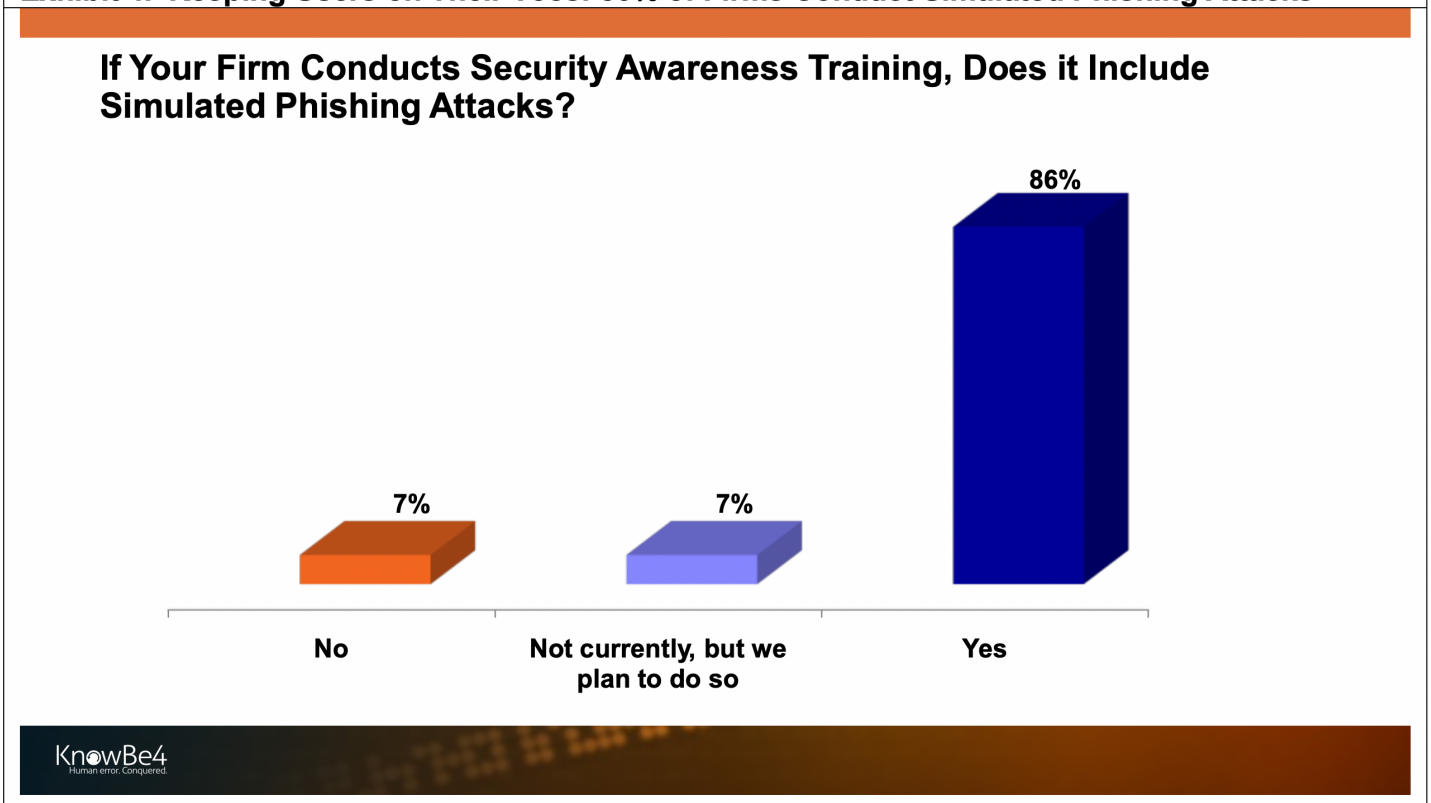
"We had been hacked several times, first time money was stolen through direct access to our bank accounts via phishing attack. The second time, several servers and desktops were locked through a phishing attack. There has not been a third time. After that second failure, every person in the organization went through in-person, multi-hour security training which is refreshed every two years. Video training and security-related emails are used on a regular basis to refresh and re-enforce this in-person training throughout the year. The biggest impact though has been simulated phishing attacks. We told everyone they were coming and even told them when they would start. We still had lots of failures. That then led to lots of re-training. After a few months though, the failure rate has decreased to the point that we really had to up our game in terms of really targeting phishing campaigns to our user base. The best part for IT is that hacks via phishing emails has been zero since we implemented this three years ago."

The CEO at a midsized IT technology services provider in Florida voiced similar sentiments. He noted the difference between a company that is lax with its security and training initiatives compared with the positive outcomes when the entire organization gets serious about security.

"…We see what a lack of security awareness does to organizations who choose not to embrace it. There is even a significant difference between customers who fully embrace the concepts and understand the true value of protecting their business, and those customers who have KnowBe4 in place, but just set it and forget it. The companies that make it a part of the corporate culture, that talk about it every day and use the tools and capabilities of the platform have the lowest percentage of security problems. From day one, the employees of these organizations understand the seriousness of what can happen and the responsibility they have to do their part in making the company secure. It has to start at the top – without C-level buy-in, the security awareness culture will never take hold."

The KnowBe4 survey respondents also revealed that nearly nine-in-10 organizations – 86% of out of the 88% that currently deploy security awareness training – also proactively conduct simulated phishing attacks. As Exhibit 4 shows, another seven percent (7%) indicated their firms do plan to implement simulated phishing attacks. This will bring the total to 95% of SAT users deploying simulated phishing attacks. These "fire drills" are an excellent means of heightening awareness and helping employees maintain a sense of alertness regarding security at all times.

Exhibit 4. Keeping Users on Their Toes: 86% of Firms Conduct Simulated Phishing Attacks



Source: KnowBe4 October 2018

A member of the IT staff at an SMB financial services firm in Ohio noted the change in the employees' attitudes from fear to empowerment following the company-mandated SAT training and regularly-scheduled simulated phishing attacks.

"At first, our users were apprehensive to the idea of monthly training. Previously we conducted the required training annually. However, since starting the monthly training along with monthly phishing, our users have commented on how they feel more informed about current security issues that benefit them professionally and personally. IT has experienced a drop in the number of PC infections."

Security Awareness Training: Tangible Results, Immediate ROI

The best thing any company can do to safeguard its data assets is to give its security and IT administrators the proper tools to educate employees so they recognize attempted hacks and phishing scams when confronted with suspicious emails. Security awareness training is an investment that will pay for itself immediately and over the long term.

The value proposition for KnowBe4.com security awareness training is that it reduces risk and lowers operational costs, management time and human error. It also does exactly what its name says: it promotes awareness among employees from the C-level executives to remote workers and employees using their own computers, tablets and mobile phones.

For overburdened companies that lack specialized, in-house security skills, security awareness training is an efficient and economical way to outsource training on the latest hacks and cyber threats. It enables organizations to reduce risk by cutting down on phishing scams by more than 80% on malware infections and phishing scams, data loss and lowering the potential for cyber-theft before it occurs. This in turn, helps to reduce ongoing operational expenditures by significantly less security-related help desk calls; reduced cleaning and re-imaging of machines; reduced down time and increased user productivity.

Corporations Give Security Awareness Training High Marks

Out of over 1,100 total survey responses, KnowBe4 received 700 anecdotal responses via essay comments and first-person customer interviews. These anecdotal responses provide deeper context and invaluable insights regarding the real-world experiences and daily operational issues confronting security and IT administrators.

The user comments were overwhelmingly positive regarding the positive impact security awareness training had on their IT departments, C-level executives and rank and file employees in recognizing and thwarting cybersecurity attacks – in particular phishing scams via email. The customer comments were culled from a wide range of vertical market segments. They included: academic (both K-12 and universities), financial, government, healthcare, insurance, legal, manufacturing, nonprofits and IT technology services. All sizes of companies were represented – from small businesses to large multinational enterprises.

An IT manager at a large state government agency in southern California that began using KnowBe4 security awareness training said it has resulted in a significant decline in successful phishing scams. *"This year, for the first year, we handed our entire yearly security training over to KnowBe4. We used Kevin Mitnick's 45-minute video, as it covered mostly everything we like to cover in our training sessions. We had the users come in and watch the video and for the interactive parts we would have the users give us their answers. We would then spend the last 15 minutes answering questions. This saved a ton of time on our end, as we did not have to turn our research into a presentation which can take weeks. Now we are using the 45-minute video for all new employees and don't have to sit with them while they watch as we can tell that they watched the video by the report on the back-end. We are also big fans of the phishing test and phish alert button in Outlook. We started at about 23% Phish-ProneTM and over time we are down under 8%. We have a lot of people using the phish alert button and have others simply asking more questions about whether an email is spam. As I tell our users, I'd rather get 100 questions a day about whether an email is legit than them clicking and getting infected. KnowBe4 has definitely made us more secure as an organization."*

The director of IT at an SME correctional supply company based in Florida also saw tangible results in the workplace – with no successful phishing incidents reported since deploying KnowBe4 security awareness training in early 2018. And he said that company employees were

putting their newfound training to good use on their home-based personal computers. *"Using KnowBe4's security awareness training has transformed our team members into a human firewall.* ***Monthly phishing penetration testing has brought our Phish-Prone rate down to 1.6%, which is well below the industry average of 12.9%.*** *We started our security awareness training in February and since then, we have managed to avoid a phishing-related security incident! We've had numerous team members thank us for providing the training, because it has impacted them at home. By raising their awareness, we've helped them avoid being taken advantage of by threat actors, both at work and at home. Here is just one testimonial from our team: So my husband is home this week; he's a teacher and on spring break. He's on his laptop in the next room, grading papers and looking at stats on the computer....and he calls me. There's a screen up on the laptop with the sound saying he has been infected and needs to call this 800 number, along with flashing screen. He called me...I shut the laptop down completely....gave him a lecture on what he opens...he swears he didn't open anything...and then I said..."I should have had you take the tutorial that Dan just made us all do. Thanks for making us do it! My computer is good. Thank you, KnowBe4, for transforming our people from potential victims of cyber threats to human firewalls!"*

A security administrator at a financial services realtor enterprise corporation in New Jersey recounted how his firm went from reactive to proactive. *"As with most corporate decisions, security awareness training was initiated by executive leadership a few years back. Ostensibly, this was a smart and forward-looking decision, but when we began to propose solutions to fill this objective, they were all struck down as too expensive. It quickly became evident that the business leadership did not seek security awareness training to improve security, but rather, to check a compliance box with our clients. Thankfully, new leadership soon took the helm and we were able to have an honest and frank discussion around our security posture (which, as you can imagine, was less than stellar). A serious investment of time, money and resources was put into a proper risk analysis. The findings would reveal some severe gaps in our security posture, not the least of which was social engineering (in particular, phishing emails). The first and fastest mitigation for this exposure, from a technical standpoint, was turning on MFA. This helped to contain the events, but did not help change the behavior that caused them in the first place. We knew we would need to provide a more robust training, but there was no flexible solution. We looked into subscribing to a video-based training service where we would send around emails to make people watch videos and run reports to ensure that had done so. So what happens? People start the training video and go talk to their friends, or shop online, or do anything but actually undergo training. We also priced out hosting live / on-site training, but given the size of the company, budget constraints would only allow us to run the program once a year. We already had training once a year. It checked a box, and nothing more. That is when we discovered the solution offered by KnowBe4. Suddenly, there were no more "nice to haves", because it had it all. Need training for the masses? Enroll all your groups for training. Need to validate the training? Test them by phishing them. Are there some individuals that seem highly susceptible to social engineering attacks based on the phishing test results? Send only those people to additional training. Oh, and the training can be a game – we're not limited to videos. This was the answer we sought. We will be going live with KnowBe4 very shortly, but just the rumor that IT security has some new product that is going to test the employees has increased the volume of phishing email reports to the help desk. I have already begun researching new hobbies to fill the newfound time I'll have not researching security events!"*

The IT manager at a midsized engineering firm in Vermont said before his company installed security awareness training, his firm was operating blind and its workers were uneducated as to the cyber threats.

"Before signing on with KnowBe4, I had no way to gauge the employees' awareness of phishing attacks and how to effectively and continually train employees to attacks. Now we have an annual refresher class that gets updated with new modules, we have a class for new hires, a class for clickers and a class

for executives. From time to time, I will add special campaigns based on the KnowBe4 newsletters. This approach has been excellent at reducing our vulnerability from 9% in 2016 to 2% or less monthly."

The CEO at midsized financial services organization in Barcelona, Spain said security awareness training has stopped successful phishing attacks.

"We use KnowBe4 training. Employees have commented on how valuable it its and that they have learned to be more careful. This has been backed up by the automated testing results we have seen go down to 0 clicks most of the time."

The CEO at SMB financial services firm in Trinidad, which recently implemented security awareness training, says she's already seen positive results.

"We have only recently started security awareness training. What I can say is that already the way I view opening suspicious emails is way more heightened. In addition, the explanations of the various types of intrusions make me more knowledgeable. Recently, we had a spear phishing attack and immediately the recipient phoned to ask the sender (me) whether I had sent the email. This is a sure sign that our employees have started to pay attention to the signs. We can't wait to learn more."

The IT security administrator at a federal government agency in Philadelphia, PA characterized security awareness training as "a complete game changer."

"The human element remains the most insecure aspect of any organization. Amazing technologies can stop all sorts of attacks, but they cannot stop your employees from sharing passwords or opening email attachments. Experts put the number at over 90% of all network breaches are only possible because of unwitting employee actions (or inactions). The most effective way to secure any organization is to take its greatest weakness and turn it into a strength. Security awareness training is the way to make employees part of the solution rather than a huge part of the problem. People do not know how they are being targeted and used by cyber criminals. It is the job of anyone in charge of an organization's cybersecurity to teach its employees how to spot phishing emails or social engineering tactics and where they should and, more importantly, should not connect to Wi-Fi. In just six months of using KnowBe4 for phishing campaigns and quarterly training, we have seen a real shift in employee mindsets. We can tell just from the questions people ask, "Is this a spam email?" or "Can I take pictures on my phone while in Mexico?" Our people no longer have their heads in the sand. They are aware of the enormity of the threat posed by life in cyberspace. We can also tell by the continuous downward trend in Phish-Prone rates. Our people are getting better, and it is simple and quick to administer. I spend more time marveling over the results than I do setting it up. It has only been about six months, and I cannot wait to see the results in another six months. It is a complete game changer."

The Cost of Security Breaches

The percentage of enterprises unable to calculate the cost of a security breach or the hourly cost of downtime consistently outpaces those that can assess the true cost of downtime over the last 10 years. That's according to several joint surveys conducted by Information Technology Consulting Corp. (ITIC) and KnowBe4 since 2008. The latest 2018 surveys, which each polled 1,000 organizations worldwide: "Security Deployment and Trends Survey and "The Hourly Cost of Downtime" found that 44% of corporate respondents said they could calculate the cost of one hour of downtime due to a security hack. However, when pressed further only half – 50% – of the 44% could make detailed downtime estimates. In actuality, only 22% of organizations, approximately one in five can accurately assess the hourly cost of downtime and the impact of a security breach on user productivity and the business' bottom line.

Fewer security incidents mean fewer calls to the help desk and less intervention required by IT/security administrators to take servers offline or perform remediation on end user systems. ITIC survey data indicates that the average cost of an IT administrator or security manager who makes an hourly wage of $50 to $60 (US) to attend to a security issue is as follows:

- Tier 1: $37 (based on a duration of up to 30 minutes of remediation performed by a single administrator)
- Tier 2: $120 to $480 (based on a duration of one to four hours involving two security administrators performing remediation)
- Tier 3: $360 to $1,800 (based on a duration of four to 10 hours and conservatively involving three security administrators fixing the issue)

The above statistics represent only the hourly labor costs associated with recovering from a security incident. Organizations must also weigh the hourly cost of downtime involving the number of knowledge workers and their specific tasks as well as the productivity impact on the business. A security breach that impacts even two key salespersons during end of month closing could have significant impact to the business, its customers and damage its reputation. The company must also calculate how many IT managers and how much time they spend on remediation efforts. When calculating total cost of ownership, organizations must also factor in the impact and cost on customers, business partners and suppliers. There is also the potential for litigation in the event any of the company's aforementioned customers are impacted by a security breach.

Hence, an organization that proactively deploys security awareness training from a firm like KnowBe4 for its IT staff and all end users will mitigate risk and increase compliance across the entire organization. Companies can use KnowBe4 to train all employees worldwide via distance learning on the same security processes and procedures and flex resources, raising awareness of the latest cyber threats and taking the necessary preventive action before disaster occurs.

Hourly Cost of Downtime

There is simply no time for downtime.
It is expensive and disruptive to productivity. Downtime for any reason – but especially as a consequence of a security breach can result in lost business, expensive litigation and cause untold damage to the company's reputation.

The latest joint ITIC and KnowBe4 Hourly Cost of Downtime Survey revealed that 98% of large enterprises with more than 1000 employees say that on average, a single hour of downtime per year costs their company over $100,000.

And an 81% majority of organizations report that the average hourly cost of downtime exceeds $300,000. Even more significantly as Exhibit 5 indicates: three in 10 enterprises – 33% – indicate that hourly downtime costs their firms $1 million or more.

Even if your organization has not experienced a security breach lasting an hour or more, a cyber attack resulting in an outage of even a few minutes can be expensive. Consider the following:

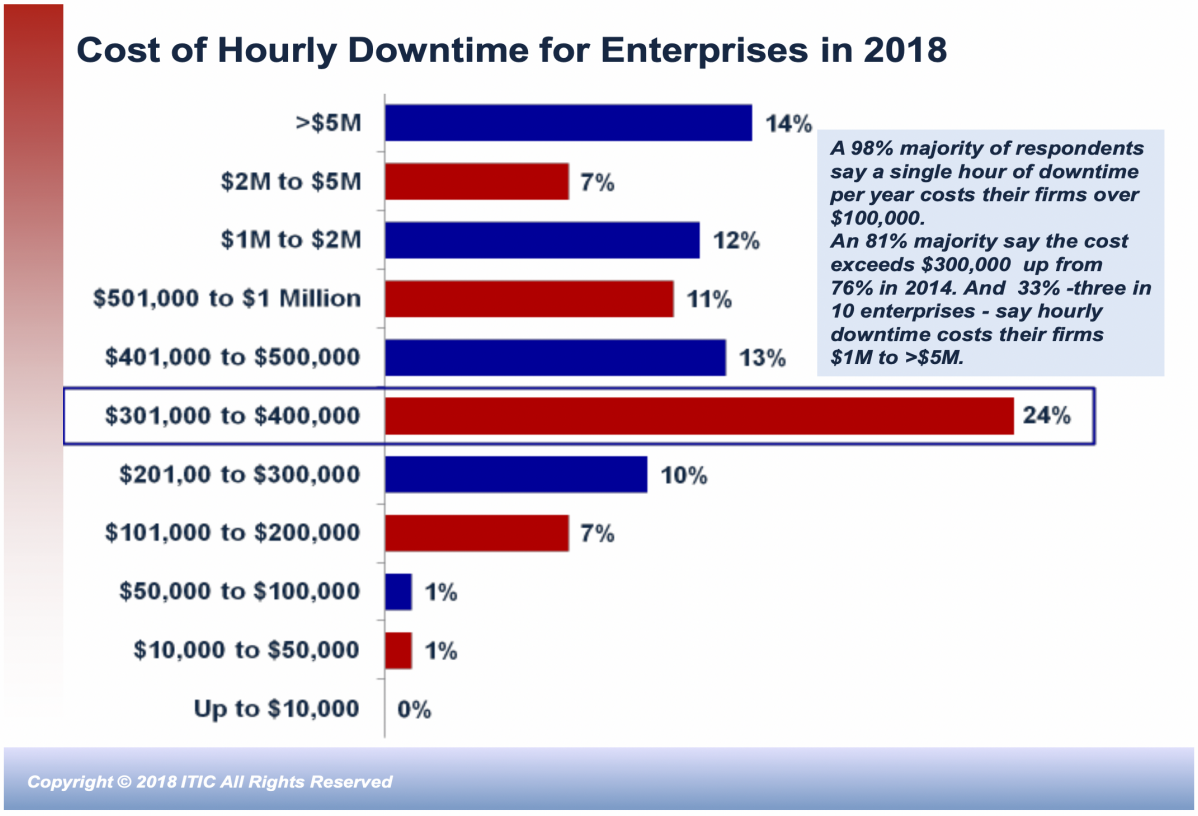
A company that estimates one hour of downtime at $100,000 (US dollars) will suffer losses of approximately $1,666 per minute. For the 24% of survey respondents who estimated that a single hour of downtime could cost their firms between $301,000 and $400,000 – the cost associated with even one minute of downtime could range from $4,998 to $6,664 per minute!

It's important to note that these statistics represent the "average" hourly cost of downtime. In a

worst case scenario – if any device or application becomes unavailable for ***any reason*** the monetary losses to the organization can reach millions per minute. Devices, applications and networks can become unavailable for a myriad of reasons. These include: natural and man-made catastrophes; faulty hardware; bugs in the application; security flaws or hacks and human error. Business-related issues, such as a regulatory compliance related inspection or litigation, can also force the organization to shutter its operations. For whatever the reason, when the network and its systems are unavailable, productivity grinds to a halt and business ceases.

Additionally, highly regulated vertical industries like banking and finance, food, government, healthcare, hospitality, hotels, manufacturing, media and communications, retail, transportation and utilities must also factor in the potential losses related to litigation as well as civil penalties stemming from organizations' failure to meet service level agreements (SLAs) or compliance regulations.

Exhibit 5.**An 81% Majority of Corporations Say One Hour of Downtime Exceeds $300K**

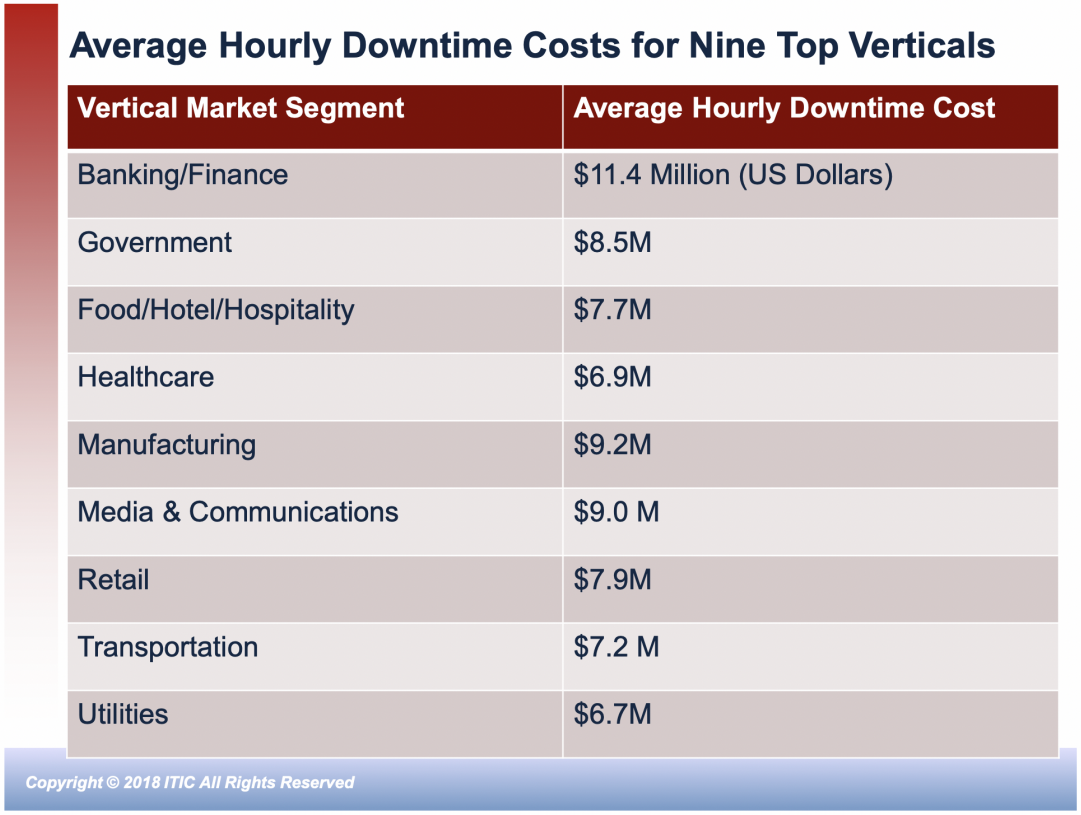


Source: KnowBe4 /ITIC October 2018

Hourly Downtime Exceeds $5 Million for Top Nine Verticals

The joint ITIC and KnowBe4 2018 Hourly Cost of Downtime Survey also revealed that for large enterprises with over 1,000 employees, the costs associated with a single of hour of downtime are much higher, with average hourly outage costs topping the $5 million (US dollars) mark for nine specific verticals. As Exhibit 6 illustrates, these industries include: banking/finance; government; healthcare; manufacturing; media and communications; retail; transportation and utilities.

Exhibit 6. **Average Hourly Downtime Costs for Top Verticals Range from Six Million to >$11 Million**



Average Hourly Downtime Costs for Nine Top Verticals

Vertical Market Segment	Average Hourly Downtime Cost
Banking/Finance	$11.4 Million (US Dollars)
Government	$8.5M
Food/Hotel/Hospitality	$7.7M
Healthcare	$6.9M
Manufacturing	$9.2M
Media & Communications	$9.0 M
Retail	$7.9M
Transportation	$7.2 M
Utilities	$6.7M

Source: KnowBe4 October 2018

Consequences of Downtime

The hourly costs associated with downtime paint a grim picture. But to reiterate, they do not tell the whole story of just how devastating downtime can be to the business' bottom line, productivity and reputation.

The joint ITIC KnowBe4 2018 Hourly Cost of Downtime Survey data revealed that although monetary losses topped users' list of downtime concerns, it was not the only factor worrisome to organizations. The top five business consequences that concerned users are (in order):

- Transaction/sales losses
- Lost/damaged data
- Customer dissatisfaction
- Restarting/return to full operation
- Damage to the company's brand and reputation
- Regulatory compliance exposure

The bottom line: it is smarter and cheaper to avoid cyber attacks and the expensive downtime, lost productivity and potential for lost, stolen or damaged data that ensues, by being proactive and deploying security awareness training.

Conclusions and Recommendations

There is no quick fix or magic formula that will guarantee 100% failsafe security.

Security is an ongoing battle that requires knowledge and constant vigilance. It will always be a work in progress. No corporation or consumer can ever declare victory.

Businesses will continually grapple with the triple threats of cost, complexity and careless end users, and they must assume responsibility for their own security.

Security awareness training can help them do that. SAT is a crucial, cost effective and efficient weapon in the ongoing war to secure the corporate data assets.

In today's interconnected digital age, it is imperative that proactive security measures be an integral part of the daily operations. No organization can hope to totally eliminate security threats and escape the attention of hacks – especially targeted hacks. However, the vigilance and knowledge gained by deploying SAT programs can thwart, identify and quickly isolate a myriad of security issues from social engineering hacks like phishing scams and bad emails. And in many instances, SAT helps employees to recognize a scam and "think before they click," thus altogether avoiding an attack. In those instances where malicious/rogue code or other social engineering security threat does manage to gain entry into the network or devices, SAT can assist in early detection and quick removal before the cyber attack can cause serious damage.

Security awareness training diminishes successful security breaches and mitigates risk to an acceptable level.

The KnowBe4 2018 Security Awareness Training and Deployment Trends Survey findings show that security awareness training produces tangible, positive results. The survey results also emphasize that companies recognize the value of SAT programs and are actively deploying them as a major bulwark against successful hacks.

To aggregate the findings:

- **64%** of respondents say **security awareness training** has helped their corporations **identify and thwart hacks** in the last six to 12 months.
- **An 86% majority** – nearly nine in 10 businesses – say security awareness training has helped to **decrease overall computer security risk**.
- **A near unanimous 96%** of respondents say security awareness training changed company Computer Security culture for the better.
- **Social engineering was the top cause of attacks, cited by 77% of respondents**, followed by malware (44%); user error (27%) and a combination of the above (19%).
- Among **businesses victimized by social engineering, some 70% of respondents said email was the root cause**; 15% were unsure.
- **88% of respondents currently employ security awareness training programs** and six percent plan to install one within six months.
- Nearly four in 10 businesses **38% – conduct simulated phishing attacks monthly**; 21% quarterly; 12% weekly; 9% ad hoc and 6% as needed.

Recommendations

It is imperative that companies and their IT departments take a proactive approach to securing and safeguarding their corporate data and assets. In the face of these well documented technology and business trends, KnowBe4 advises organizations of all sizes and across every vertical market segment to:

- **Take inventory** Know what devices are on your network and what versions of software your users have on their myriad of desktops, notebooks, tablets and smart phones.
- **Deploy security awareness training** from the boardroom down to the mail room.
- **Conduct phishing attack tests** on a regular basis and randomize the attacks.
- **Stay current** on the latest security patches and fixes.
- **Ensure that C-level executive management** takes a leadership position in all security initiatives.
- **Devote the necessary time** to providing ALL employees with security awareness training.
- **Check and confirm the security of ALL third parties** who access your corporate network and data assets. This includes trusted third-party consultants.
- **Budget appropriately.** Security can no longer be practiced in hindsight.
- **Regularly review and update computer security policies.**
- **Conduct a thorough remediation** in the wake of a phishing attack or a security breach of any kind, no matter how short. It is essential that security and IT administrators be able to identify the type, duration and severity of the attack in order to determine the extent, if any, damage and to eliminate the source of the vulnerability.
- **Calculate the hourly cost of downtime and business impact of security breaches.**

Organizations should conduct regular security audits of their entire server hardware and server OS and application infrastructure to determine vulnerabilities and compare and contrast the security of their various platforms. The ability to adhere to compliance standards and meet service-level agreements (SLAs) hinges on the security of all of the systems, devices (including bring your own device) and applications across your entire ecosystem.

There is no substitute for performing due diligence. Corporations should also construct pilot networks well in advance of any deployment to simulate their intended production environment as closely as possible and check for any potential security holes. Customers should also avail themselves of their respective vendors' technical support and technical documentation, particularly with respect to the timetable for regularly scheduled security patch releases. It is imperative that businesses apply the applicable security patches as they become available. There are also many security-related hardware and application compatibility sites and forums. These provide invaluable detailed guidance to avoid problems and troubleshoot technical issues.

It's also crucial that businesses actively scan security sites such as National Institute of Standards and Technology (NIST). It's important to perform regular scans of news and media outlets for any new reported vulnerabilities and remain current on patches. Customers should also contact their OEM and third-party hardware and application ISVs, systems integrators and consultants for the latest security information and familiarize themselves with security and overall systems requirements. Organizations should also prevail upon these vendors to disclose any known issues or incompatibilities and, if any exist, when they expect to issue patches.

Methodology

KnowBe4.com conducted the 2018 Security Awareness Training Deployment and Trends Survey which polled 1,100 businesses during August and September 2018.

The independent web-based survey included multiple-choice questions and essay responses. KnowBe4 received 700 detailed essay comments and conducted one dozen phone and email interviews with Security administrators, IT managers and C-level executives. The essay comments, coupled with the in-depth, first-person interviews provided us with invaluable anecdotal data. The interviews and essay comments validate the survey responses and provide deeper insight into the security issues challenges confronting corporations in both the immediate and long term.

To deliver the most unbiased, accurate information, there was no vendor sponsorship for the online poll or the subsequent first-person interviews conducted in connection with this project. We also employed authentication and tracking mechanisms during the survey data collection to prevent tampering and to prohibit multiple responses by the same parties.

Respondents were culled from 48 vertical market segments. The top five vertical market sectors in order were:

- Financial
- Government
- Healthcare
- Manufacturing
- IT Technology/Services Provider

All sizes of companies were represented. Some 40% of the participants were SMB firms with one to 20 servers; 34% came from midsize and smaller enterprises with 21 to 100 servers and 28% of survey participants hailed from large enterprises with 101 to over 5,000 servers. The survey was global. Some 80% of respondents hailed from North America compared with 20% of international respondents.

Appendices

Verizon 2018 Data Breach Investigations Report
https://www.verizonenterprise.com/verizon-insights-lab/dbir/

AT&T 2017 Global State of Cybersecurity, Mind the Gap: Cybersecurity's Big Disconnect.
https://soc.att.com/2pCKw8x

Hackmageddon 2017 Cyber Attack Statistics
https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/

Revision Legal 2018 Data Breach Statistics
https://revisionlegal.com/data-breach/2018-statistics/

Wired Magazine "The Worst Cybersecurity Breaches of 2018 So Far," July 9, 2018,
https://www.wired.com/story/2018-worst-hacks-so-far/

ITIC/KnowBe4 2018 Hourly Cost of Downtime Survey Report
ITIC/KnowBe4 2014 – 2015 State of Corporate, BYOD and Mobility Security Trends Survey
ITIC/KnowBe4 2013 – 2014 Security Deployment Trends Survey Report

Train Your Staff Today

Ready to start phishing your users? Find out what percentage of your employees are Phish-prone with your free phishing security test. Plus, see how you stack up against your peers with the phishing Industry Benchmarks! You can accomplish the same dramatic end results of the study with KnowBe4's Phishing Security Test (PST).

Additional Resources

Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

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

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

About KnowBe4

KnowBe4 is the world's largest 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.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make better security decisions.

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