KnowBe4
Human error. Conquered.

KNOWBE4 2019

Security Threats and Trends Report

October 2019

Table of Contents

Executive Summary

The yearly, independent, KnowBe4 2019 Security Threats and Trends Survey polled 600 organizations worldwide mid-2019 on the major security issues they will face in the next 12 to 18 months.

A majority of corporations—86%—have proactively amplified security initiatives over the last year to combat the increase in cybersecurity attacks. Nearly nine out of 10 businesses—89%— say they're currently better equipped to deal with security threats than they were in 2018.

However, organizations still face significant challenges when it comes to their security initiatives. Three quarters or 76% of organizations say the biggest and most persistent security threat comes from "the enemy from within"—careless end users—who regularly clicks on bad links, placing organizations at higher risk of falling victim to email phishing, ransomware, CEO fraud scams and various forms of malware. And 58% of organizations cite budgetary constraints as an ongoing challenge in upgrading security.

Of the 89% of respondents who say that their firms are more prepared to cope with security threats, 36% say they're "much better equipped." However, a 53% majority of those polled more cautiously characterize their companies as "somewhat more prepared," than they were 12 to 18 months ago, and added the caveat that "we need to do more to secure our environment." Only a six percent minority believed that their firms were less prepared to deal with security issues in 2019 than they were the same time a year ago.

KnowBe4's latest survey results find that enterprises are well aware of the need to fortify security and safeguard data assets and intellectual property in light of various cybersecurity threats. These include but are not limited to: viruses and malware; sophisticated email phishing and CEO fraud scams—aka Business Email Compromise;— social engineering; password attacks; denial of service attacks; data leaks; open ports on servers and routers; targeted attacks by hackers; corporate espionage; attacks at the network edge; lost and stolen devices; and lack of security on employer and employee-owned bring your own devices (BYOD).

A near unanimous 96% of organizations say that email phishing scams pose the biggest security risk, followed by 76% who identify end user carelessness and 70% of respondents who cite social engineering as the biggest security threats facing their firms over the next 12 months (**See Exhibit 1**). And in a nod to the growing sophistication of the organized hacking community, nearly half or 46% of respondents fear their organizations may fall victim to a targeted attack. This is an increase of 11 percentage points from the 35% of organizations that perceived targeted hacks as a danger in KnowBe4's 2014 Security Threats and Trends Survey.

Among the other survey highlights:

- Despite the well-documented increase in cyber threats, 43% of KnowBe4 survey participants still don't allocate a significant portion of their IT budgets towards security expenditures (**See Exhibit 3**). One-third or 30% of respondents don't have a separate security budget and another 13% say the organization's security budget is less than $25,000 annually.
- Only 14% of organizations say they're concerned about insider attacks from internal employees.
- Half—50%—of participating companies report their security and IT staff are overworked and 40% say their organizations will face a shortage of skilled security professionals within the next 12 months.
- An 82% majority of respondents say proactive security maintenance (e.g., installing upgrades

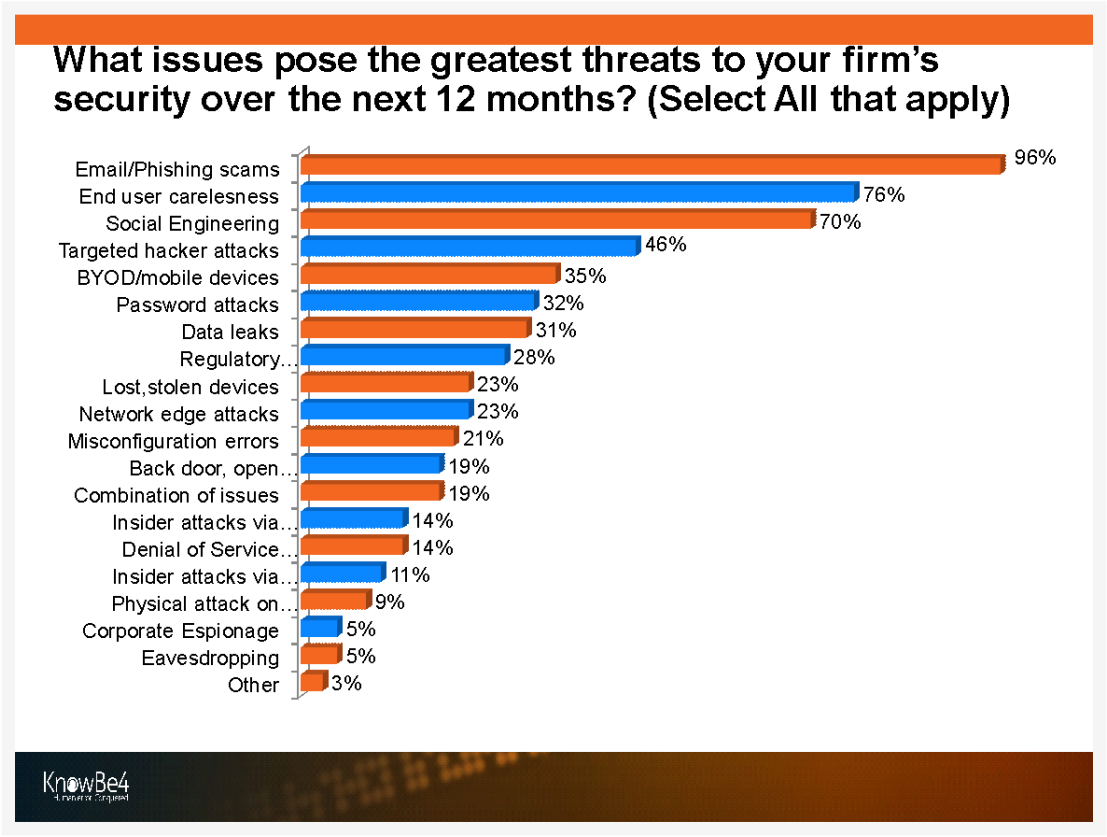
and patches) is a top priority over the next 12 months. That was followed by 61% of organizations that cite the need to keep pace with the latest security threats and 61% that say updating and enforcing computer security policies is major concern for their organization.

- Some 27% of respondents identify their organizations' inability to identify, quickly respond to and shut down hacks over the next 12 months as a top challenge and source of concern.
- Only 18% of organizations calculate the hourly cost of downtime related to security hacks.
- A 53% majority allow employees to access the corporate network and data using BYOD. However, only 39% of organizations currently have a plan to respond if a BYOD such as a laptop, tablet or smart phone is hacked, stolen or lost.

The KnowBe4 survey responses also underscore the importance of upgrading security and training internal security and IT administrators as well as end users. Hackers are continually upping their game. As **Exhibit 1** below illustrates, organizations must contend with and defend their devices and networks against a wide array of security threats.

EXHIBIT 1

Organizations Cite phishing scams, end user carelessness and social engineering as top security threats



Source: *KnowBe4 2019*

The KnowBe4 2019 Security Threats and Trends Survey presents a comprehensive picture of organizations' most pressing security issues and challenges over the next 12 to 18 months. It also offers actionable insights, via anecdotal essay comments and first-person interviews with C-level executives as well as IT and security administrators as to how organizations intend to proactively

defend their data assets from hackers going forward.

Data and Analysis

The KnowBe4 2019 Security Threats and Trends Survey results indicate that the overwhelming majority of organizations and their security and IT departments recognize the increasing danger posed by the growing number of cyber threats. And they are aggressively taking countermeasures to mitigate those threats.

The top three threats that respondents say pose the most danger are: email-based scams (e.g., phishing, ransomware and CEO fraud); end user carelessness and social engineering. This is not surprising because these three issues—along with BYOD and mobility—are inextricably intertwined by the common thread of the "human element."

The KnowBe4 study delved into organizations' most pressing security issues and challenges via essay comments and first-person interviews with C-level executives as well as IT and security administrators. Those conversations revealed that organizations of all sizes across a wide range of vertical markets are extremely concerned about budgetary constraints and the dearth of skilled IT administrators and resources necessary to secure their environments at a time when hacks are more targeted and pernicious.

The anecdotal data also suggests that IT and security administrators continue to find themselves caught in the crossfire between C-suite executives and end users. Security and IT departments must convince upper management to allocate the monies and resources to purchase security packages and security awareness training to safeguard their environments. At the same time, IT and security managers must police the organization's end users and instill a sense of urgency regarding the importance of being vigilant regarding security practices in the face of everyday threats such as phishing scams, malware, ransomware, sextortion emails and rogue code.

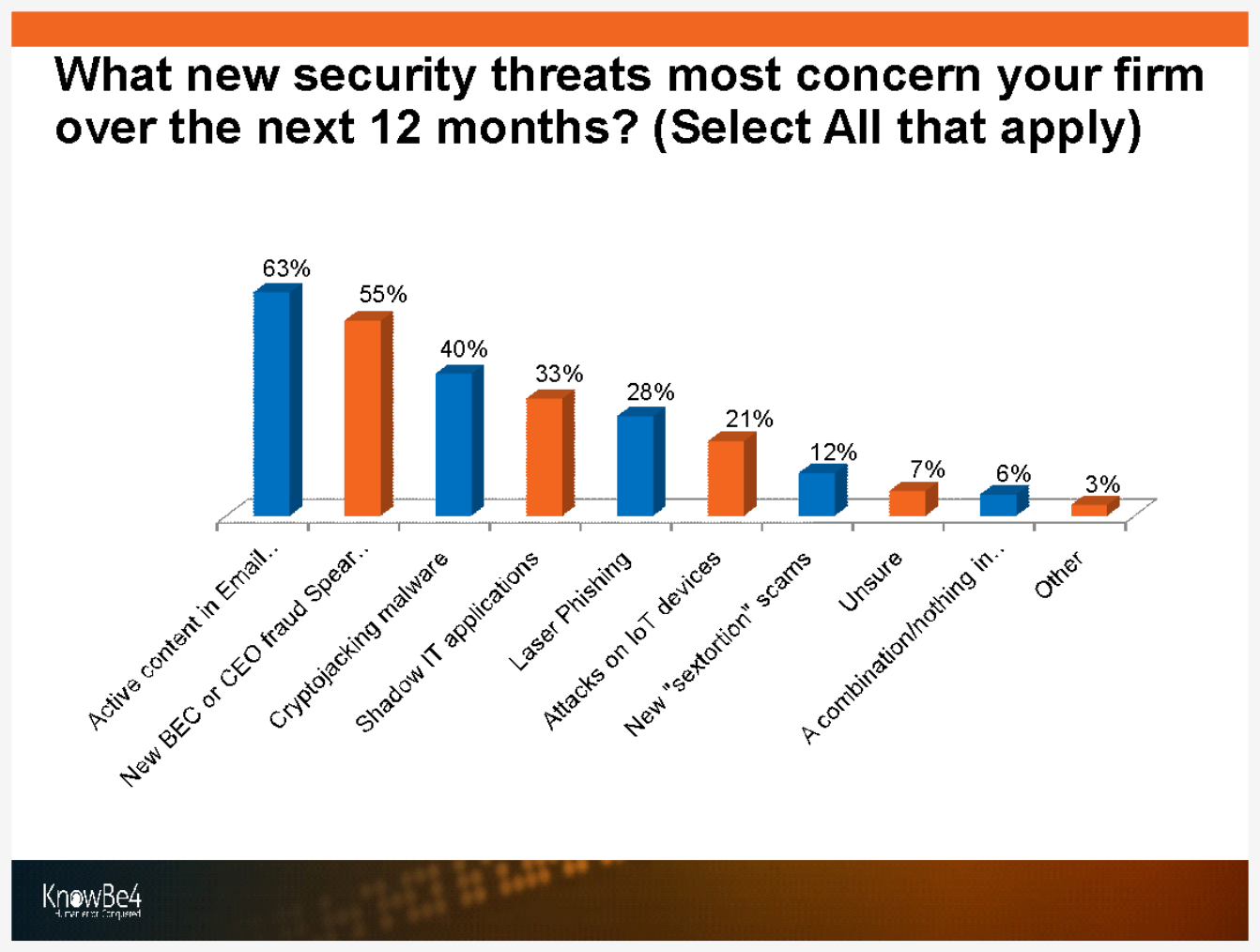
Careless End Users, Lax Security Policies and Tight Budgets Fuel Cyber Crime Success Rates

The increasing frequency and high success rate of email-based cyberattacks have organizations understandably on edge. This trend has been evident in all of KnowBe4's surveys since 2013. KnowBe4 survey respondents directly attribute the high degree of successful email cyberattacks into their organizations on the willingness of end users—including management—to click on bad links without thinking. Other culprits include weak computer security policies, lax enforcement and a lack of IT budget dedicated to purchasing security devices and software, hiring security professionals and getting security awareness training (**See Exhibit 3**).

As **Exhibit 2** illustrates, the results of KnowBe4's 2019 Security Threats and Trends Survey show that email-based hacks are among the most prevalent and dreaded of cybercrimes. They are also among the most successful.

EXHIBIT 2

Email Phishing, CEO Fraud Scams Top Companies' List of Security Threats



Source: *KnowBe4 2019*

KnowBe4 survey respondents accept the reality that cyber threats are a fact of computing life in the digital age. They are nonetheless rightfully concerned that they have little knowledge about when and where the next threat will present itself. Most concede that it's a matter of "when not if" their organizations will get hit.

The network administrator at a mid-sized law firm near Washington, D.C., that has nearly 100 servers, summed up the sentiments of many IT professionals.

> *"The whens and wheres of cyberattacks are unknowns, and I'm particularly worried about the next attack vector we don't know about yet," he says.*

KnowBe4 survey participants gave extremely detailed and insightful responses regarding their security safeguards and preparedness. During interviews with KnowBe4 analysts, many security and IT administrators described how they've adopted a multi-layered approach that pays particular attention to what they typically regard as the weakest link in the network ecosystem: end users.

An IT staff member at a federal government agency in California that spends $1 million to $4.9 million annually on security says his organization has developed a thorough security framework with "limited resources, but an unlimited procurement policy."

> *"We've achieved this level of security with an approach that boils down to one overarching principle: Defense-in-Depth, from the network to the endpoint. We have firewalls, both external and internal. We have SIEMs, including Alienvault, Splunk and Qradar.*
>
> *We have deployed multiple anti-malware solutions, including ESET, MalwareBytes, and Cylance, on a number of our servers and endpoints. We have real-time traffic monitoring tools that help us manage the infrastructure, and other tools to monitor data as it travels through the network. We have spotted ransomware and stopped it in its tracks.*
>
> *We have MAC-level, 802.1x authentication on switches and APs. We run virtual environments on thin clients throughout 99% of our agency. Any compromised image gets eliminated from the virtual server and replaced with a fresh image. Each of those endpoints, in turn, run various levels of software-based endpoint protection; you can't even plug a USB without us knowing about it. Policy wise, we require two-factor authentication to use internal resources. We restrict access to social media and personal emails during work hours on our domain, but they have access on a separate external network, not connected to the main domain, that they're free to use at their own risk. But all of this begins with the end user; arguably the most challenging part of securing an environment.*
>
> *Running KnowBe4 campaigns as part of our security framework has given us the ability to assess the risks associated with email attacks and act accordingly. Staff [members] who repeatedly click on emails undergo security awareness training. Thanks to this product [KnowBe4], our last campaign reported the lowest click rate since the start of our campaigns, nipping a notoriously weak link in the bud."*

As **Exhibit 3** illustrates below, security budgets remain tight for many organizations. Nearly one-third or 30% of respondents say that their organizations do not have a security budget that is separate from their annual IT capital expenditure budget. Some 13% indicate they allocate less than $25,000 on security spending and 12% spend $25,000 to $50,000 annually on security.

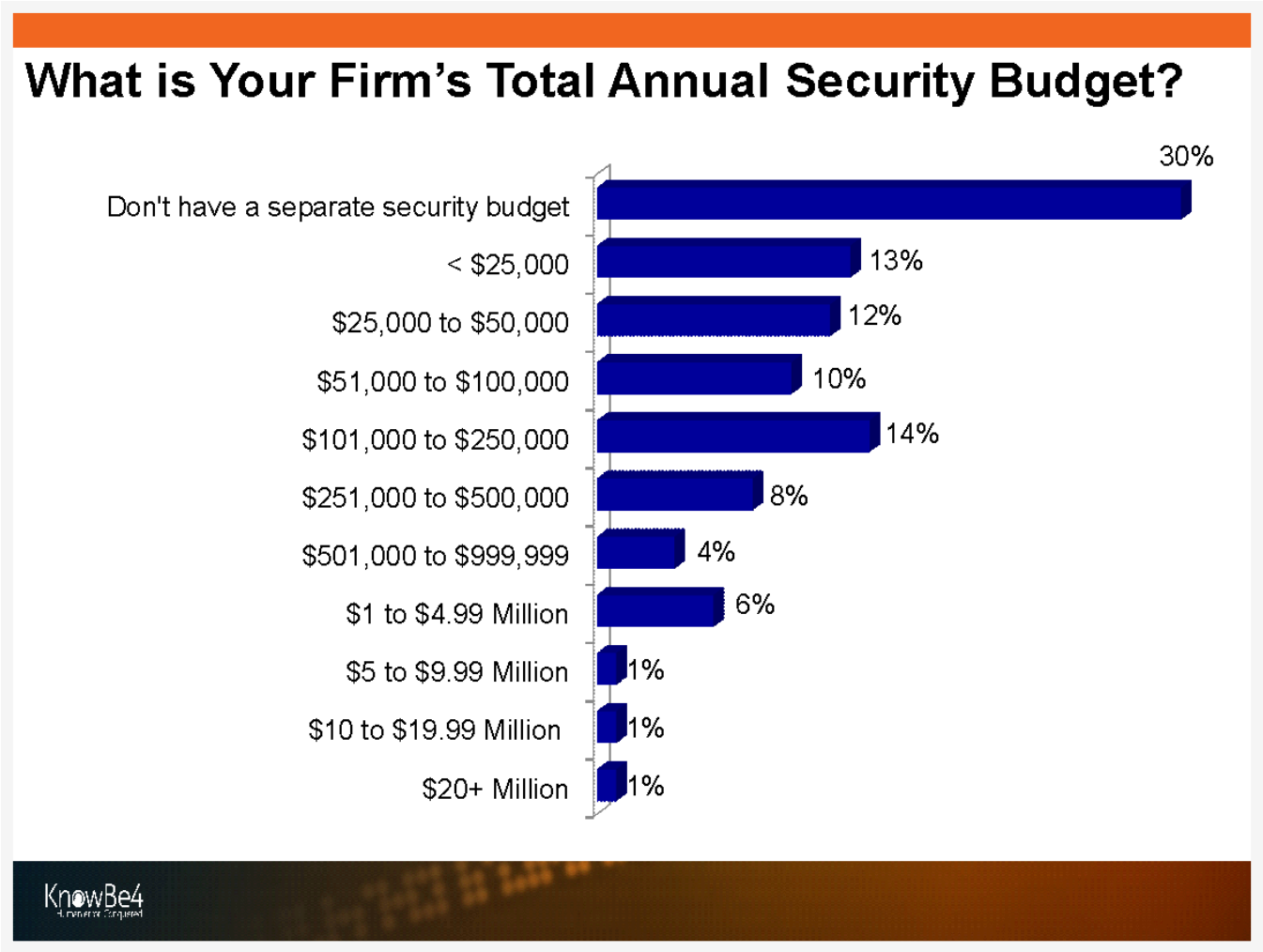
Fifty percent of the organizations polled dedicate less than or up to $50,000 a year to purchase security products, software or security awareness training despite the well-documented rise in all types of cyberattacks and cybercrimes.

Still, this marks an improvement in security spending over KnowBe4's 2018 Security Awareness Training Deployment Trends Survey, which polled 1,100 organizations. That survey found that 34% of respondents did not have a separate security budget; 16% spent less than $25,000 on security and 13% of respondents allocated $25,000 to $50,000 on annual security spending.

Although the fact that 50% of organizations spend less than or up to $50,000 annually on security products and training, that's still an improvement over the KnowBe4 2018 survey results that found 64% of organizations spent $50,000 or less every year on security.

EXHIBIT 3

Security Budgets Tight: 50% of Firms Spend Less than $50K Annually



Source: *KnowBe4 2019*

Dedicated security spending or budgets are crucial as users detailed in their anecdotal essay comments and first-person interviews because they often make the difference between the IT department's ability to be proactive versus reactive.

That is the situation for a systems administrator at an SMB financial services firm in the Southeastern U.S., who says his company has no separate security budget.

> *"Being a small company, sadly most everything we do here is reactive. We have virtually no IT budget. So no, I don't think we have a good approach to security, other than running manual scans and patching what we can."*

An IT manager at a mid-sized retailer in California who spends less than $25,000 on security says his business is challenged by a lack of security funds.

> *"Security for our organization continues to be challenging. A lack of specific skills and training in*

IT security requires us to rely on partnerships with vendors. We continue to hope they are keeping up their responsibility for keeping the organization safe. We often think about a more formal relationship with an MSSP."

The IT manager at an Auckland, New Zealand government enterprise organization that also has no separate security budget, expressed his concerns. He notes that the lack of funds contributes to his IT staff being overworked; his inability to hire skilled security personnel and inadequate funding for security awareness training.

"We have a three-year cycle of investment to uplift security technologies and have added another staff member to the team in the last nine months. We are in the process of motivating [upper management] to add a third member to the security team. We understand that we need technology, trained and skilled people, and processes and awareness training to ensure that our organization's security improves over the next few years. It is a marathon not a sprint; as long as we focus our efforts on the most critical threats first."

Most survey respondents though, fell in the middle of the spectrum. That is, although they weren't awash in security funds, they were nonetheless very proactive and believed that their organizations had made progress in the last 12 to 18 months.

Such is the case of a network architect at a K -12 school district in Iowa, who says he's adopted a straightforward approach to security.

"We are a public school system and have very limited resources and a limited technical staff, so a simple plan works best. We train our users with KnowBe4. This has significantly cut down on users clicking on scam emails.

We keep all hardware/software up to date no matter how difficult it becomes. Patching firmware and software is a security requirement, period. The last thing is monitoring using NGFW's and rule-based monitoring of end user behavior. This is our simple, easy to follow security process. Like the old saying goes, 'keep it simple stupid.'"

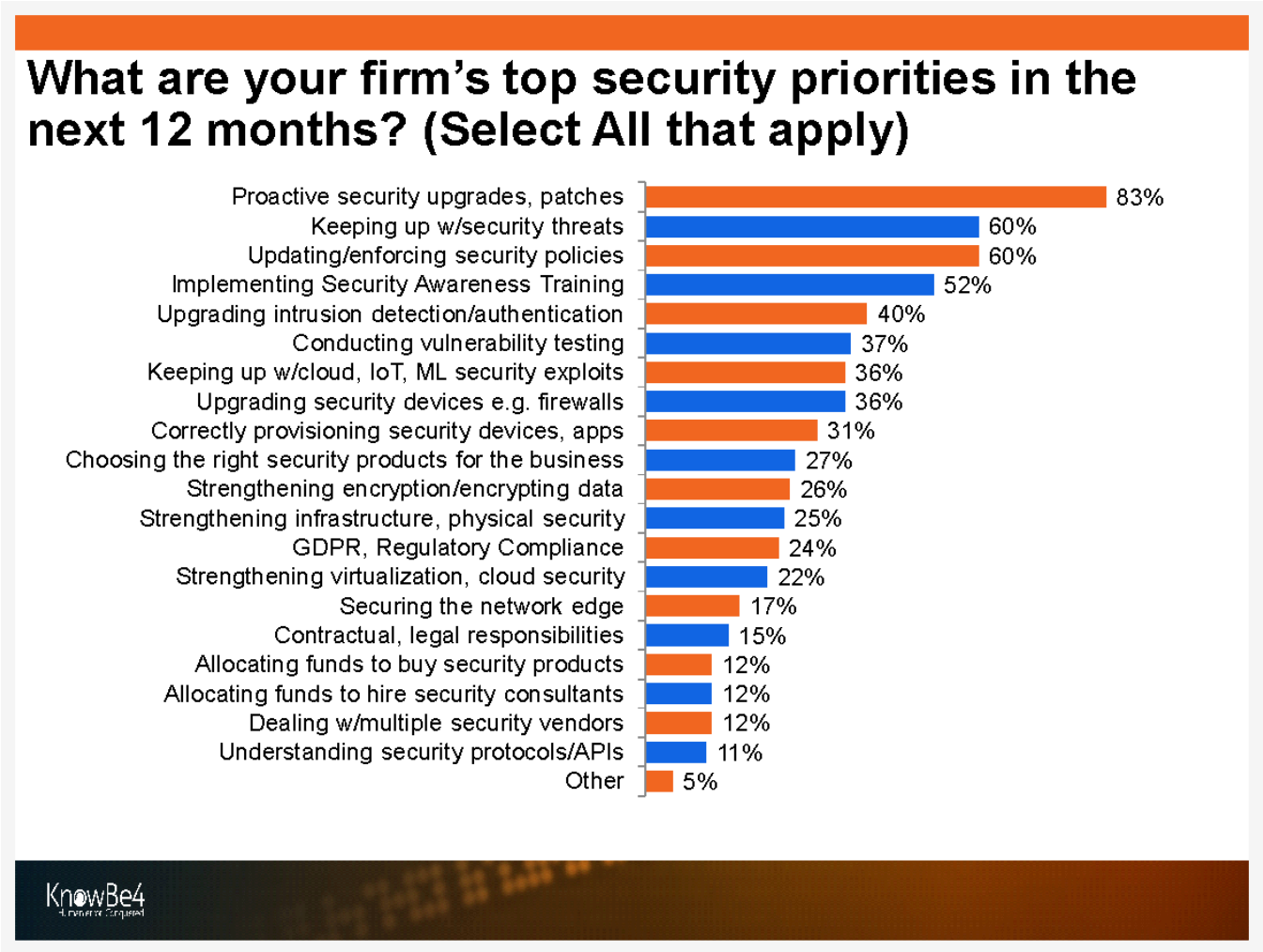
Users' Top Priorities: Daily Security and IT Vigilance

The KnowBe4 study results also reinforced the fact that vigilance in daily IT and security operations is crucial, particularly with respect to keeping pace with routine operational management and security tasks.

As **Exhibit 4** indicates, security professionals and IT administrators are extremely concerned with the pragmatic issues that most directly impact their end users' daily computing life and routine. Organizations' top security priorities in the next 12 months are: performing proactive security upgrades and patches, cited by 83% of respondents; keeping pace with the latest security threats; and updating and enforcing security policies, both of which were cited by 60% of survey participants.

EXHIBIT 4

Upgrades, Enforcement and Training are Top Security Priorities



Source: *KnowBe4 2019*

Additionally, over half—52%—of organizations say implementing security awareness training for IT departments and end users is high on their list of priorities.

Four-in-10 organizations say that upgrading intrusion detection and authentication mechanisms is a top priority, followed closely by 37% of respondents who cite vulnerability testing as a key part of their security strategy in the next 12 months. Thirty-six percent of organizations say that keeping up with technology hacks involving IoT, migrating to the cloud and upgrading security devices like firewalls are priorities. Another 31% say correctly provisioning devices and applications is a priority and 26% referenced strengthening encryption/encrypting data. All-in-all, these types of tasks comprise much of a security and IT professional's daily and weekly activities. And like everything security-related, these professionals must stay up to date to keep pace with the ever-evolving threat landscape.

This explains why security awareness training initiatives have assumed a much more prominent and pivotal role in organizations' security strategies in recent years, with 52% of survey participants saying it's a priority for them. This is up from the 41% of respondents in KnowBe4's 2013 survey who cited security awareness training education as crucial for their security operations.

Security awareness training makes sense on many levels. First and foremost, users are and likely will continue to be the weakest links in corporate security defenses. Security awareness training also yields tangible results. The return on investment (ROI) is immediate according to the anecdotal data KnowBe4 received in essay comments and first-person customer interviews. Security and IT professionals were unanimous in stating that security awareness training greatly reduced the number of successful email-based cyberattacks like phishing, BEC, CEO fraud and ransomware hacks against their organizations.

The chief information security officer at a large government agency in Mississippi with 100-250 servers that spends $250,000 to $499,999 annually on security, just assumed her role in the last six months. She found that the organization's security was reactive and set about changing that by using a multi-faceted strategy.

"I'm currently on a fast track to learn the security solutions we have and I've also been working on policies and compliance. In addition, I'm implementing an incident response plan and two-factor authentication. I want to take the organization from reactive to proactive/prevention mode. We use the KnowBe4 security awareness training and it has helped us reduce our threats by 50% in the first year."

The security administrator at a mid-sized healthcare organization in the Midwest also takes a proactive approach to security to adhere to regulatory compliance laws and says that security awareness training plays a pivotal role in their security initiatives.

"We are taking a much more proactive role in security now that our staff has grown, and we have more time to do so. We are subject to HIPAA for some of the data that we house so have always taken security very seriously. We are confident in our hardware and software regarding security and view employees as the weakest part of our security. We employ KnowBe4 to train them and also send email regarding current events in the security world. Our policies are ever-changing and evolving as the environment around them changes. Another challenge not listed above is keeping our office culture the same while improving security."

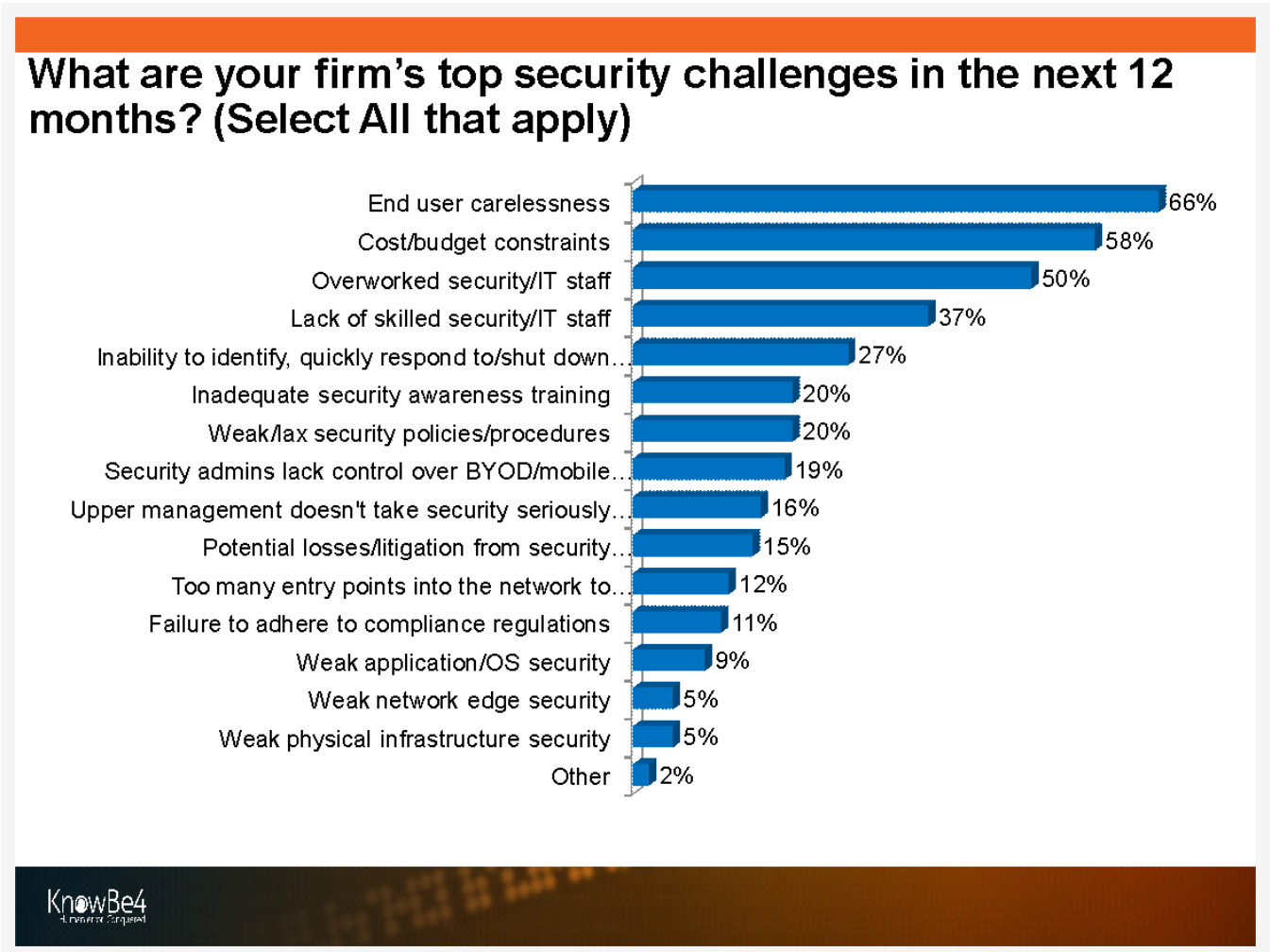
Toughest Security Challenges: Reining in End Users; Getting More Budget and Hiring Skilled IT and Security Staff

The category of top security challenges in many ways mirrored the biggest security threats facing organizations and their security and IT departments over the next 12 months. Once again, the responses were similar. As **Exhibit 5** illustrates below, the top three most challenging security issues in order are: end user carelessness (66%); cost/budget constraints (58%) and overworked security/IT staff (50%).

Interestingly, respondents were not as concerned about less pressing topics such as potential losses or litigation arising from security litigation or data theft (15%); too many entry points into the network (12%); failure to adhere to compliance regulations (11%) weak network edge (5%) and weak physical infrastructure security (5%).

EXHIBIT 5

Toughest Security Challenges: Careless Users, Tight Budgets and Overworked Security/IT Staff



Source: *KnowBe4 2019*

The IT manager at a New Jersey-based mid-sized law firm that has no separate security budget says the paucity of funds places his company at higher risk of attack. He's particularly worried about the threats posed by email, phishing scams and end user carelessness. The IT manager is also concerned by the potential for the corporate network to get infected when the law firm's attorneys insert clients' USB devices into the company's computers. It took a brush with disaster to get management to loosen the purse strings.

"For years, I've been trying to educate management as to the need for user training in the way of cybersecurity. Money has never been made available and I had been reduced to developing ineffective in-house brochures and emails to address this need. However, that all changed when a user decided to use a third-party application in order to virtually install a program on his laptop to use. Both the third-party app and the program were not approved by our organization. Even though the user only had basic rights on his laptop, the application managed to launch a rogue program that corrupted over 60% of his system files.

If it weren't for our malware detection hardware from Carbon Black, our network could have been compromised. As it was, the infection was cataloged before he [the user] reconnected the laptop to the network. Thus, we were able to isolate the laptop before any further damage was done. The laptop, however, required a complete rebuild. I used this opportunity to once again drive home to management the need to invest in a security awareness program to educate our users. Within 30 days, we purchased KnowBe4 and it is already yielding great results."

Conclusions and Recommendations

In today's interconnected digital age, it is imperative that proactive security measures be an integral part of the daily operations. No organization can completely eliminate security threats and escape the attention of hackers—especially targeted hacks. However, the vigilance and knowledge gained by deploying security awareness training programs can thwart, identify and quickly isolate myriad security issues from social engineering hacks. The latest BEC and CEO frauds, phishing, ransomware and sextortion scams are increasingly sophisticated. They manage to dupe intelligent, experienced users and even government agencies into taking the bait and clicking.

To reiterate, there is no such thing as 100% foolproof security. But multi-layer security defenses, bolstered by security awareness training can lessen the number of successful security penetrations and mitigate risk to an acceptable level.

Frequent security training also helps employees to recognize scams and "think before they click," and potentially avoid an attack. In those instances where malicious/rogue code or other social engineering security threats do manage to gain entry into the network or devices, SAT can assist in early detection and quick removal before the cyberattack can cause serious damage.

The KnowBe4 2019 Security Threats and Trends Survey findings, anecdotal essay responses and first person customer interviews underscore the fact that organizations, security professionals and IT administrators recognize the value of SAT programs and actively deploy them, particularly as the first line of defense against email phishing scams, CEO and BEC frauds and ransomware attacks, that end users routinely and thoughtlessly click on, on a daily basis.

To reiterate, there is no such thing as 100% foolproof security. But multi-layer security defenses, bolstered by security awareness training can lessen the number of successful security penetrations and mitigate risk to an acceptable level.

Methodology

The **KnowBe4 2019 Security Threats and Trends Survey** polled 600 organizations mid-year 2019.

The independent web-based survey included multiple-choice questions and essay responses. To supplement the survey data, KnowBe4 conducted over one dozen first-person phone and email interviews with security professionals, IT managers and C-level executives. The anecdotal data obtained from these customer interviews validates the survey responses and provides deeper insight around the security and the real-world business issues facing organizations. The subjects covered include topics like budgets and cost constraints, keeping pace with the latest security threats, finding the right products and tools for the business, educating end users and the challenges associated with finding skilled IT and security professionals to staff IT departments.

To deliver the most unbiased, accurate information, KnowBe4 did not accept any vendor sponsorship money 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 party.

Respondents were culled from 40 vertical market segments. The top five vertical market sectors in order were:

- Financial
- Manufacturing
- Healthcare
- IT/Services Provider
- Non-Profit

Organizations of all sizes were represented. Some 44% of the participants were from SMB organizations with fewer than 200 employees; 26% came from midsize and smaller organizations with 201 to 500 end users and 30% of survey participants were from large enterprises with 500 to over 10,000 workers. Some 78% of respondents hailed from North America compared with 22% of international respondents. The countries represented by global respondents include: Australia, Belgium, Brazil, Canada, China, Denmark, Egypt, Germany, India, Ireland, Italy, Japan, Mexico, New Zealand, Netherlands, Poland, Spain and South Africa.

Additional Resources

Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

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 address 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