KnowBe4
Human error. Conquered.

WHITE PAPER

The 2019 What Keeps You up at Night Report

WHITE PAPER: The 2019 What Keeps You up at Night Report

Maintaining organizational security against cyberthreats last year was a unique challenge. Cybercriminals turned up their execution a notch – targeting specific industry verticals, organizations, and even individuals. Increases in the frequency of ransomware, phishing, and cryptojacking attacks were experienced by businesses of nearly every size, vertical, and locale. Many criminal organizations now leverage the very same types of machine learning AI to help them better understand how to improve the art of their attack.

2018 was also a year of some of the most sensational and successful attacks. Marriott's 500 million stolen customer records represented the largest data breach in history, reminding organizations that no company is completely safe. Over 184 million ransomware attacks occurred, with damages estimated at over $8 billion. And phishing attacks are now being used to commit fraud that has some businesses out millions of dollars.

And in the midst of all this cyber-turmoil, IT organizations have been tasked with trying to establish and maintain a layered security defense that protects the organization and its users, despite the ever-changing threat landscape. Much of the constant barrage of threats, attacks, malware, and news stories has got to have some IT organizations deeply worried.

So, we wanted to find out which of these issues are keeping you "up at night"; that is, which aspects of security – from prevention, to attack, to detection, to response – are you most concerned about.

In this report, we're going to take a deep dive into the stuff of nightmares - security concerns that have organizations worried. The report will focus on six areas of concern:

- Attack Types
- Security Initiatives
- Compliance Security
- User-Related Issues
- Resource Issues
- Executive-Level Concerns

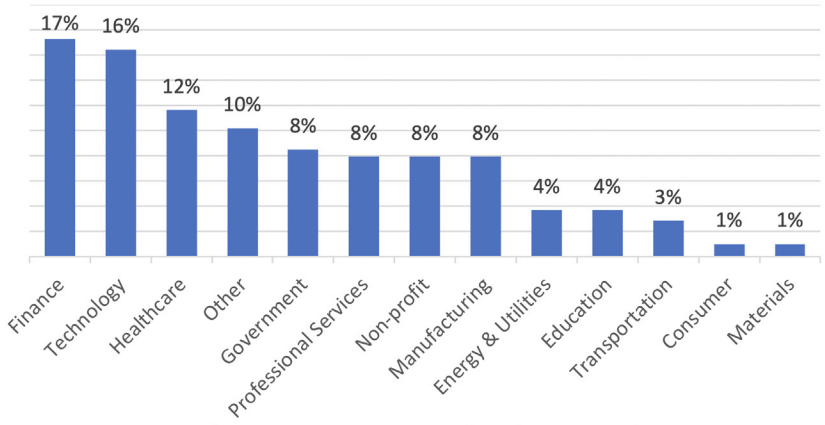
We'll dig into each area, providing insight into what parts of security have organizations lying awake in their beds, and which ones allow them to sleep soundly.

There was a 70% overlap between organizations with no proper security culture in place and those organizations having major concerns with negligent users.

About Our Respondents

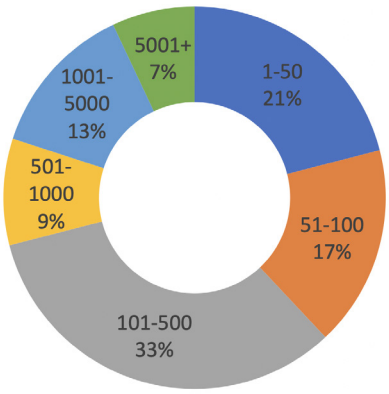
Over 350 organizations globally participated in this year's report.

The top six industry verticals represented in this report are shown below. The other industries included Insurance, Construction, Real Estate, and more, each contributing less than 1% of the total respondents.

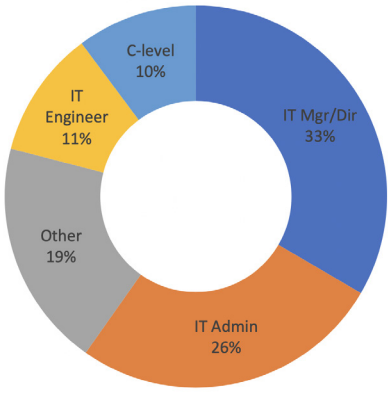


% of participating organizations by industry vertical

Respondents provided us with a broad representation of organizations of every size, gaining perspective from a wide range of IT titles, ranging from IT admin all the way up to those in the C-suite.



Breakdown of respondent by org size



Breakdown of respondent by title

Key Findings

This data in this report highlights the areas around security that organizations don't quite yet have a handle on. While a portion of organizations had many of the issues under control, **on average, 81% of organizations were concerned to some degree** about a security issue we raised.

Below is a list of the top issues keeping organizations "up at night":

Users are the primary concern for **92%** of organizations. Negligent users that become phishing attack victims tops the "up at night" list.

Ensuring security is in place that meets **GDPR** requirements is still a challenge for **64%** of organizations, despite the regulation details being out for quite some time.

Security awareness training along with phishing testing topped the list of security initiatives **80%** of organizations are needing to implement.

Data breaches remain a rampant problem worldwide. With executives concerned about breach repercussions, this one has **95%** of organizations worried.

Attackers utilization of **compromised credentials** is such a common tactic, **93%** of organizations are aware of the problem, but still have lots of work to do to stop it.

Nearly every part of the success of a security strategy relies on having **adequate budget**, a material concern for **75**% of organizations.

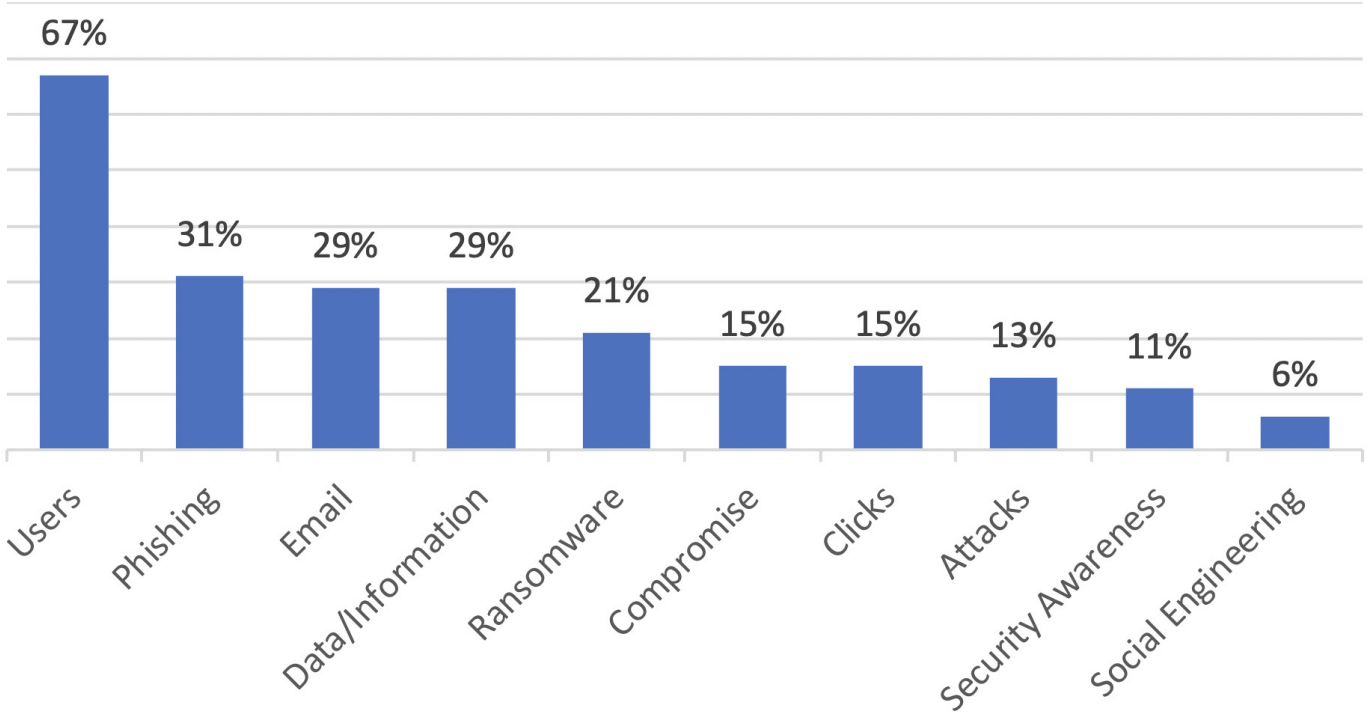
What's Keeping IT Up at Night?

We started by asking our respondents the open-ended question, "What single issue around your organization's security stands out as the greatest concern that either figuratively or literally keeps you up at night?". The responses range from single-word answers like "ransomware" and "users" to long paragraphs with detailed explanations about circumstances they face. To provide some insight into their responses, we thought we'd display the answers as a word cloud, with word size indicating frequency across all our respondents.

The negligent user is the single largest concern to organizations within this report.

We found that most respondents are concerned about the combination of negligent or careless users and their impact on the organization when phishing and ransomware attacks. Compromised credentials, breached data, and access to the corporate network all topped the list of repercussions. Equally of interest was establishing a corporate sense of user-centric security awareness.

Below is a list of the 10 keywords that appear most often and the frequency at which they were mentioned as a concern.

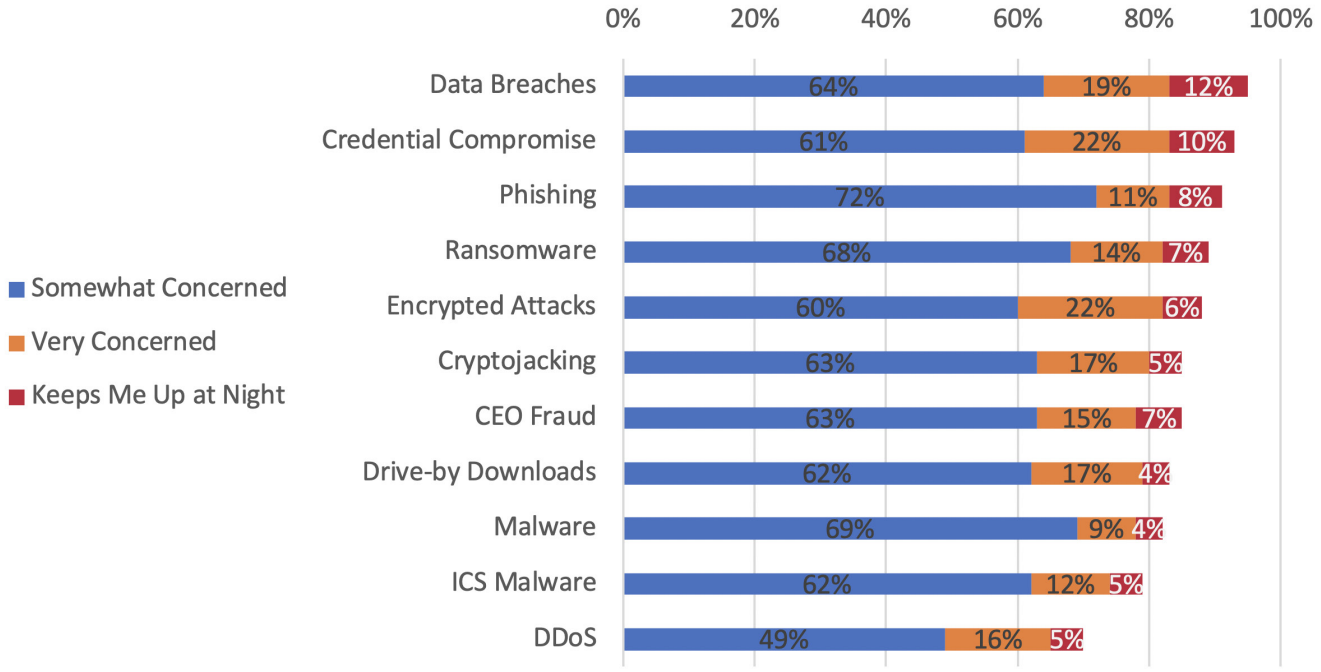


Concern #1: Attack Types

Organizations today have a large number of attack vectors to prevent, monitor for, detect, alert to, and remediate. With cybercriminals getting so good at their craft, it's difficult for organizations to focus on just one issue. So, which attacks are a concern? We broke the issue of attacks down into 11 pressing types:

- CEO Attacks / Whaling
- Credential Compromise
- Cryptojacking
- Data Breaches
- DDoS
- Drive-By Downloads
- Encrypted Attacks
- ICS Malware
- Malware
- Phishing / Spear Phishing
- Ransomware

The chart below breaks out the levels of concern around each attack shared by organizations.



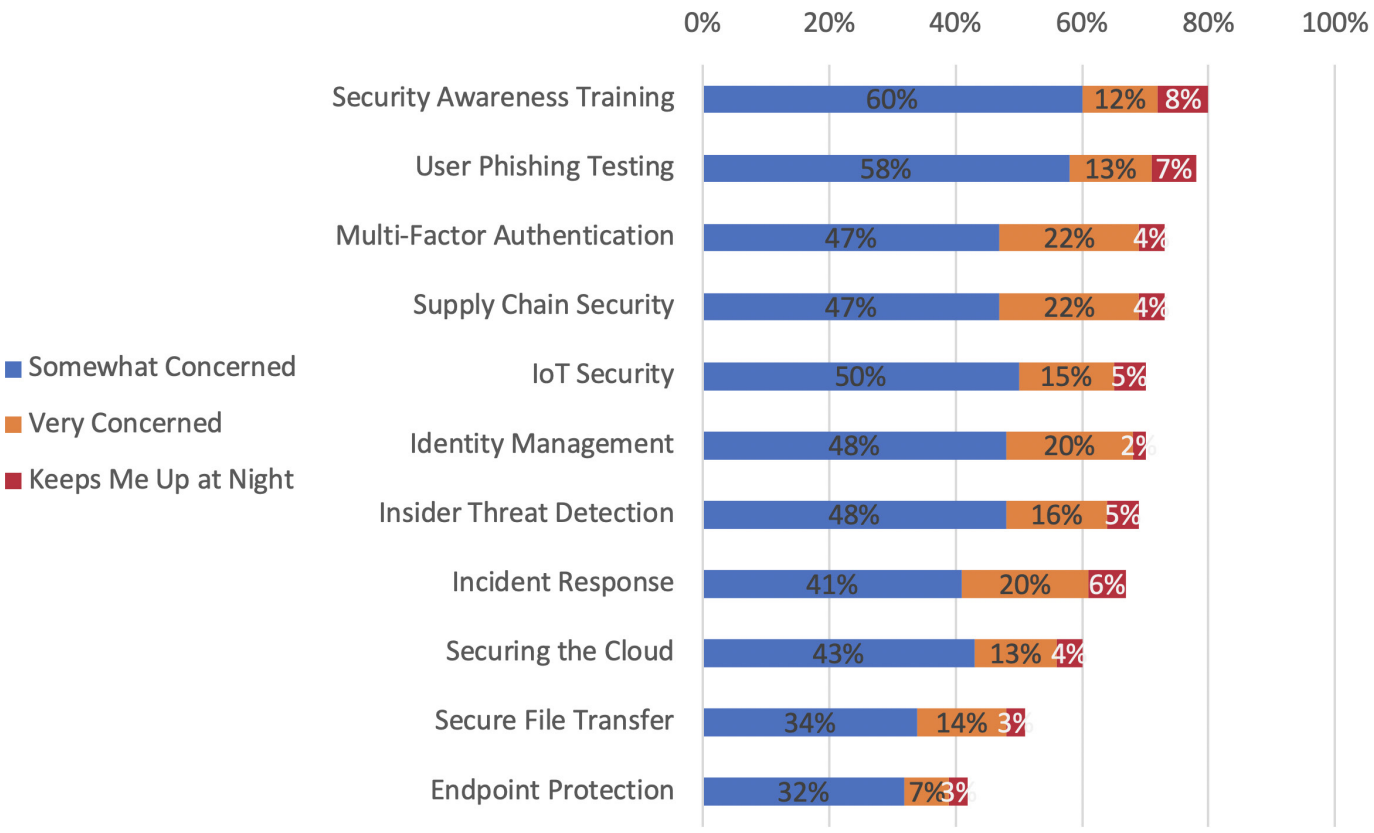
You'll notice that nine of the 11 attack types have over 80% of organizations concerned to some degree, and a near alignment between the issues most keeping IT up at night with overall concern.

Data breaches were the primary issue most organizations are concerned about, with credential compromise coming in as a close second. These two issues go hand-in-hand, as misuse of credentials remains the number one attack tactic in data breaches, according to Verizon's 2018 Data Breach Investigations Report. Phishing and ransomware ranked next, demonstrating that organizations are still not completely prepared against these relatively "old" attack vectors.

Concern #2: Security Initiatives

Having a layered security strategy in place can make the difference between knowing you have your identified risks addressed and being very concerned with no idea what to do should an incident occur. While most organizations are aware of the need for a layered security strategy, not every one of them has it implemented. So, which security initiatives are still an issue?

We asked about 11 common aspects of a layered security strategy. The chart below shows the level of concern around implementation of each security initiative for those indicating they do not have a current implementation in production.



On average, 42% of organizations have one or more of these initiatives completely implemented, with organizations utilizing and average of three initiatives. But, it's the use of a layered security strategy – that involves using multiple types of solutions at various parts of an attack – that provides the greatest levels of protection. For example, of those organizations with seven or more initiatives in place, none of them found any of the 11 previously listed attack types either very concerning or keeping them up at night.

Concern #3: Compliance

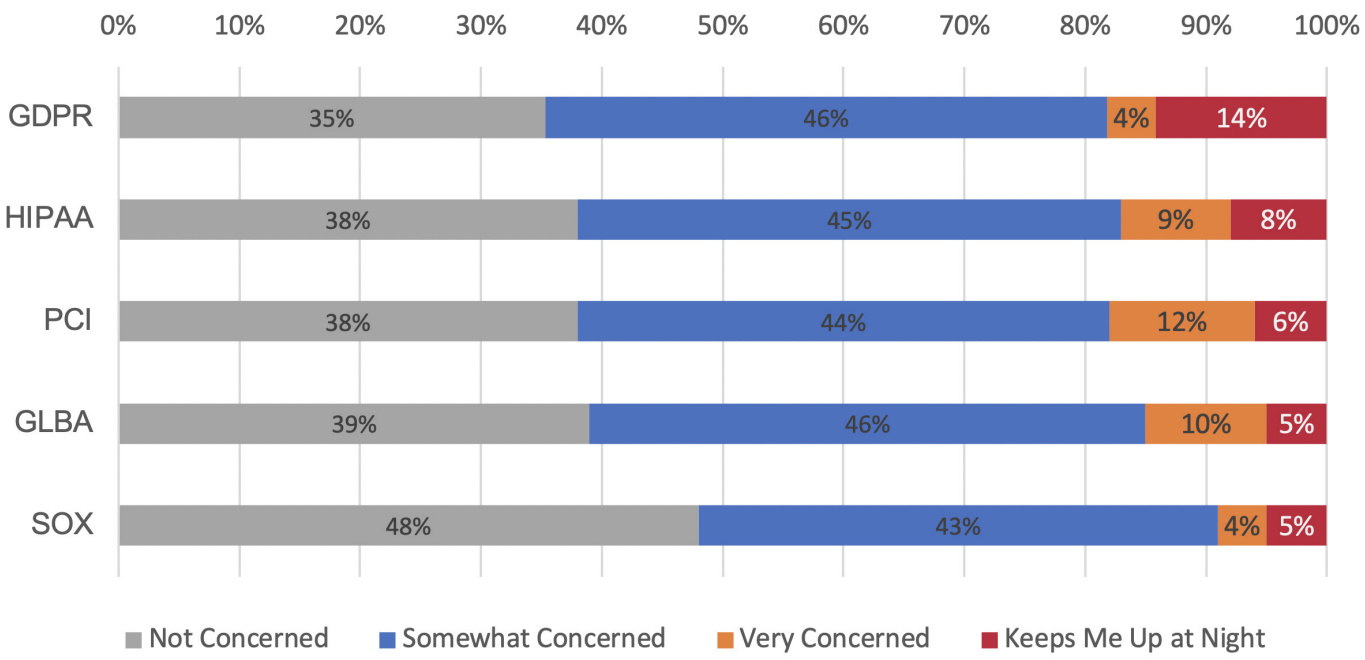
Nearly all compliance mandates today have some data security standard included. And, while most directives provide no real specifics (with the exception of PCI), the issue of establishing and maintaining appropriate levels of security that some auditor or governing body will approve of is a challenge at best. But which ones do organizations have a grasp on, and which ones are still not completely compliantly secure? We asked about five of the most pressing compliance standards:

- GDPR
- GLBA
- HIPAA
- PCI
- SOX

To provide more color, the answers we provided were:

1) We have security addressed / Not Concerned
2) Compliant security is an on-going issue / Somewhat Concerned
3) We have serious work to do / Keeps Me Up at Night
4) Working to establishing compliant security / Very Concerned

The chart below shows the breakout of concern levels for organizations that indicated they are subject to each compliance mandate.



The majority of organizations had some degree of concern, no matter the compliance mandate. In addition to the compliance mandates above, some government organizations noted needing to be Criminal Justice Information Services (CJIS) standards, several financial services noted needing to meet SEC and FINRA requirements, and a number of organizations representing several industries needing to adhere to NIST 800-53 standards. None of them denoted an inability to meet these standards.

Concern #4: Users

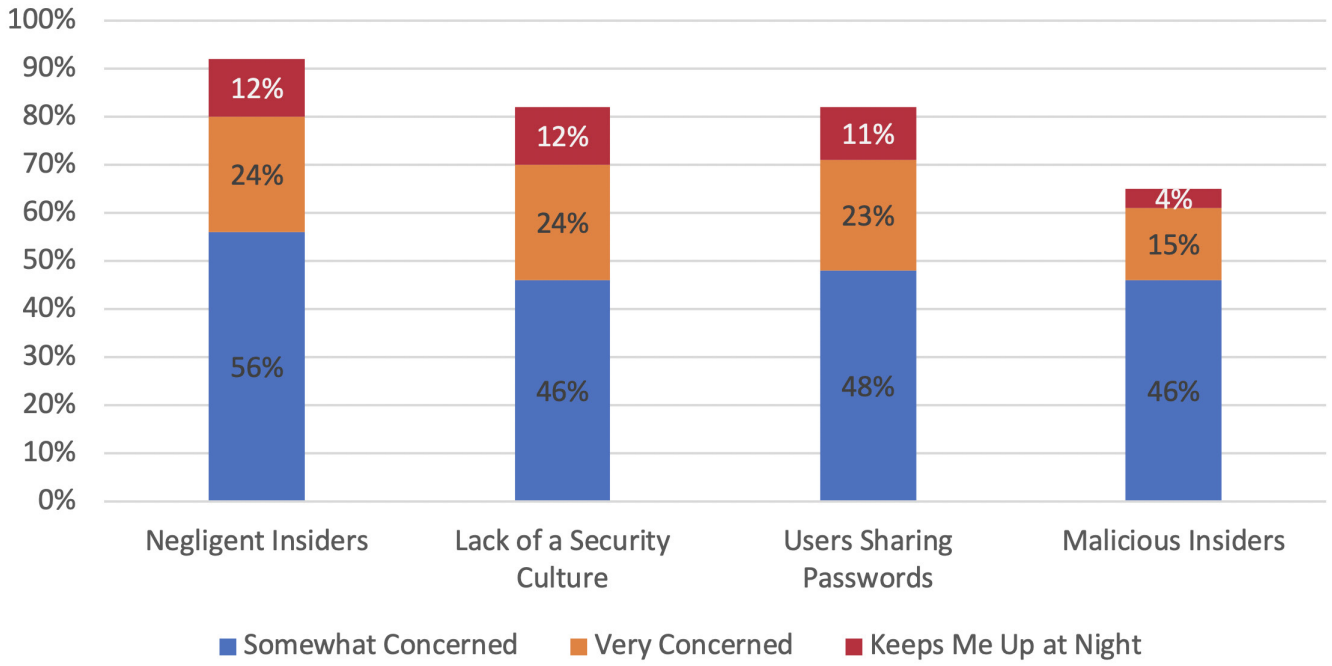
One of the most common themes among our initial open-ended question on concerns was the issue of users. Because users interact with attack assets – such as emails, links, attachments, webpages, and more – they become both part of the attack and your defense strategy. So, where along that spectrum do organizations see their users?

To find out, we sought to inquire about four specific scenarios involving users:

- Negligent Insiders / Phishing Victims
- Malicious Insiders
- Users Sharing Passwords
- A Lack of a Security Culture

As shown below, the negligent user is the single largest concern to organizations within this report. This finding coincides with the top three open-ended concern answers we received – users, phishing, and email. These users are unaware of the dangers that lurk within email and on the web, putting organizations at risk.

We also see that a lack of a security culture and users sharing passwords tied for a very close second place, with a nearly equal percentage of organizations kept up at night as with user negligence. Malicious insiders, while still a material concern, however ranked materially lower than that of the negligent user.



We found these concerns to be evenly distributed across organizations of all sizes and industry verticals, indicating every organization shares the same frustration with user risk.

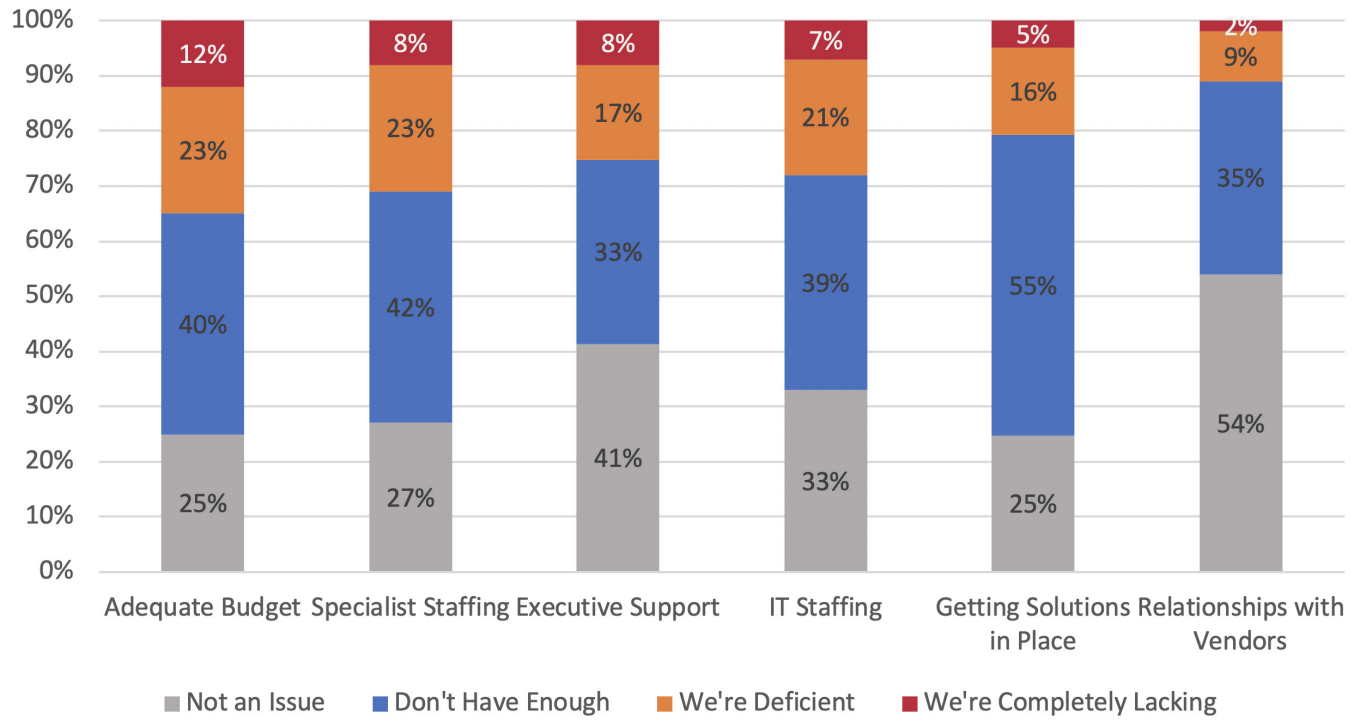
Concern #5: Resources

One of the sources of IT problems is often the lack of resources. Nearly every concern we've raised so far in this report is normally attributed to some kind of resource deficiency – whether it be budget, staffing, internal expertise, executive support, relationships with vendors, or having the right solutions.

So, we wanted to understand where IT organizations lacked the proper resources. We focused on five common issues plaguing IT. We offered the following choices to characterize the issues:

1) Not an issue / Not concerned
2) We don't have enough / Somewhat concerned
3) We're deficient on this / Very concerned
4) We're completely lacking / Keeps me up at night

The chart below shows the majority of organizations have issues across the board, with the greatest overall resulting challenge being putting proper solutions in place.

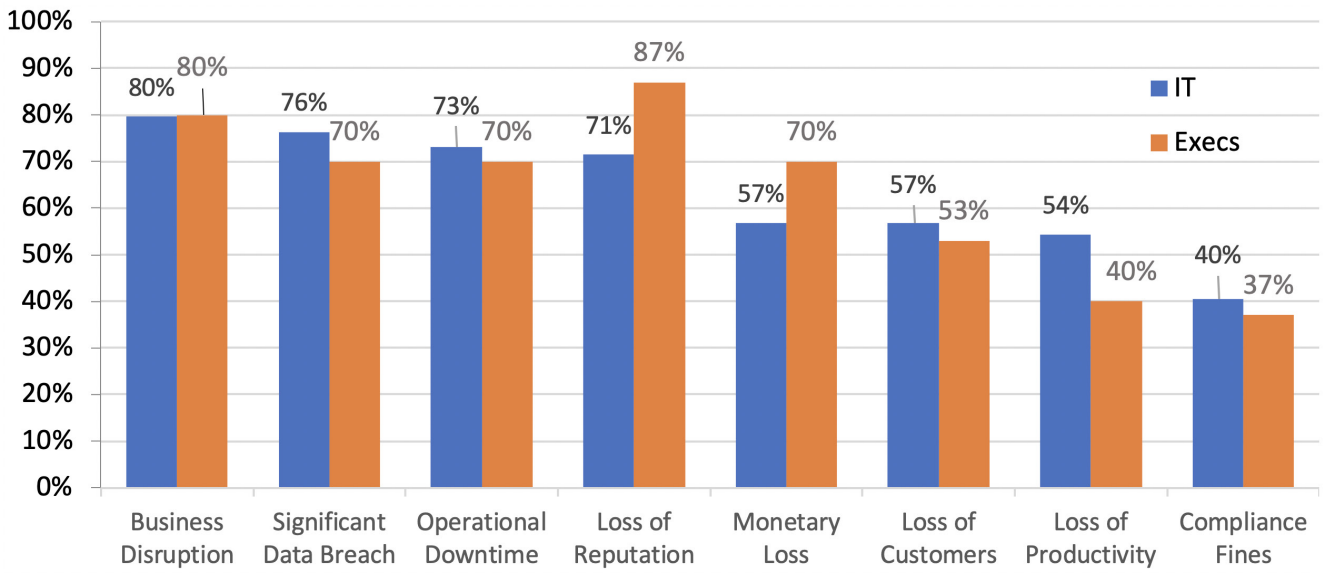


Budget was the top "up at night" concern. Of those citing a lack of budget, the average organization had less than two of the 11 security initiatives in place and elevated levels of concern across nearly all of the areas covered in this report. Deficient executive support tied with specialist staffing as the second place "up at night" another factor playing a role, with 61% overlap between organizations with a lack of budget and those with lacking executive support.

Concern #6: Executive Issues

The C-suite of any organization is thinking at a much less tactical level and is more concerned with issues that keep the business from running as normal. We asked which business issues are of concern to the executive level of the organization.

The data shown below breaks out the responses by those indicating their role in the organization as an executive and those indicating a lower-level IT position. As shown, by and large, IT staff understand the concerns of their executive team rather well, with most concern levels from IT staffers closely matching that of the respondents indicating themselves as executives.



Reputational and monetary losses were materially higher concerns for executive respondents than projected by IT staffers, making loss of reputation the number one concern for executives Loss of productivity was far less of a concern by IT staffers, with operational downtime's level of concern remaining fairly consistent between IT staffers and executive respondents.

Getting a Good Night's Rest

This report provides insight into the areas of IT security that are simply put – an issue. But it doesn't need to be that way. Based on the report findings, many of your organizations are all experiencing the same challenges. In many ways, the problem may simply be a disconnect between the technology you know you need, and the business requirements your executives are focused on. Take a look at the high-level steps below – these provide some guidance on how to best approach the issues keeping you up at night.

1) Have a Security Strategy – An average of 46% of you are "working" on security initiatives, but don't have a clear plan. Planning out a layered security strategy is the first step.

2) Get Executive Buy-In – 59% of you don't have enough support. Educate your executive suite on the security challenges you're facing in business terms they understand. Discuss the plan you wish to put in place and how it helps uphold the executive concerns mentioned in this report. Lastly, cover the potential business repercussions to the organization should security not be made a priority.

3) Obtain Necessary Budget – A massive 75% of you don't have the budget necessary. Using your plan, prioritize what's needed to execute the strategy, and leverage the executive buy-in you have.

4) Implement a Security Culture – The largest concern in this report by and far is that of negligent users. The desire is to get users to stop entertaining phishing scams, clicking on links, opening documents, and providing credentials to fake websites. It starts with establishing a security culture. There was a 70% overlap between organizations with no proper security culture in place and those organizations having major concerns with negligent users.

You can put all the security solutions in place that you want, but if your users are still going to click every link that comes into their inbox, you're still at risk. Implement security awareness training and user phishing testing to elevate your employee's understanding of the need to incorporate security as part of their job function. This will make them a part of the defense and lower organizational risk.

It's probably safe to say that one or more of the security concerns raised in this report keeps you up at night. By working through the steps above, you will find your organization far more protected and yourself sleeping through the night.

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 organisations 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 organisation with security top of mind.

Tens of thousands of organisations 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