KnowBe4
Human error. Conquered.

WHITEPAPER

The 2020 What Keeps You up at Night Report

UK Edition

Table of Contents

ABOUT THIS REPORT

Maintaining organisational security against cyber threats today is a unique challenge of trying to hit an always moving target with a toolset that's trying to keep up. Cyber criminals are focused on the targeted game; identifying specific industry verticals, organisations, and even individuals, and devising tailored scams and attacks to maximise success. In addition, we're seeing increases in frequency, sophistication, and scope of ransomware, phishing, business email compromise, and malwareless attacks.

We're also watching cyber attacks evolve. Ransomware has grown to include data theft and extortion to increase the chances of successful attack. The use of deepfake audio is now being used to trick users over the phone, and attackers are no longer satisfied with raking in thousands of dollars when millions are plausible.

In response, IT organisations have been tasked with establishing and maintaining a layered security strategy that protects the organisation and its users. But the ever-changing landscape of threats, attacks, and malware has some IT organisations deeply worried.

So, we wanted to find out what's changed since we initially published this report last year. While last year's report covered the globe, this year's results are broken out into geographical reports. In this report, we're seeking to understand which issues are keeping UK organisations "up at night"; that is, which aspects of security—from attacks, to security initiatives, to risks, to organisational constraints—are respondents most concerned about.

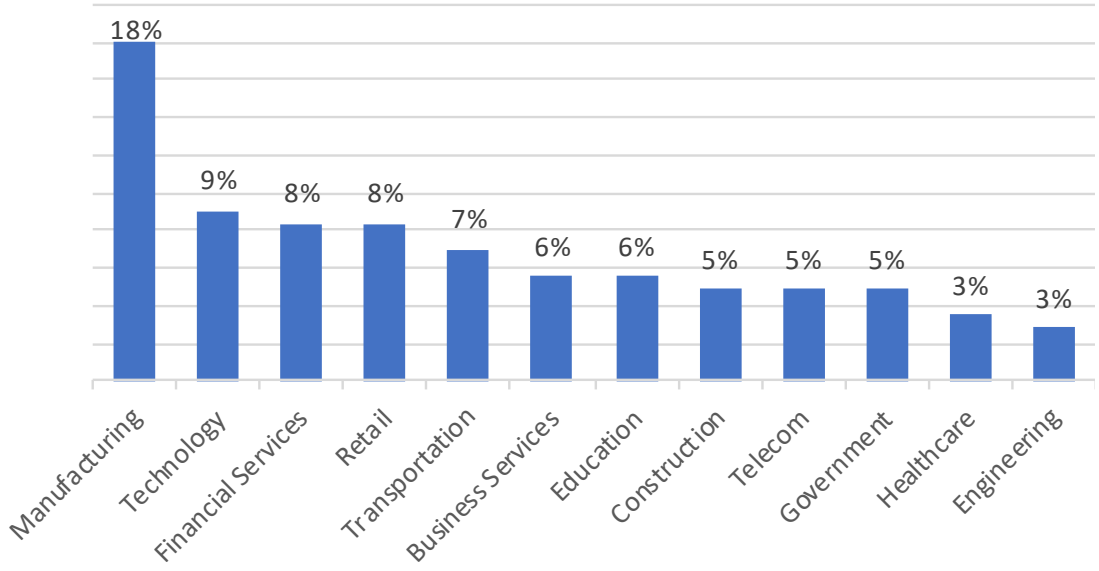
In this report, we're going to look at the state of security from six perspectives:

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

Each provides insight into just how prepared UK organisations are today and how that preparedness impacts the need to be concerned about common cyber risk that exists today.

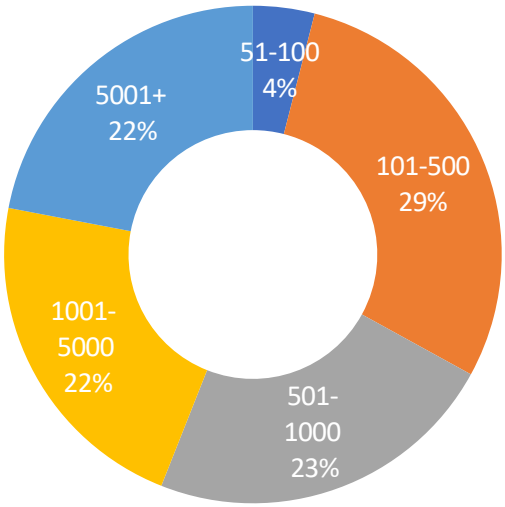
ABOUT OUR RESPONDENTS

Nearly 200 organisations across the UK participated in this year's report. The top twelve industry verticals represented in this report are shown below. The other industries included Insurance, Automotive, Biopharma and Biosciences, Communications/Telecom, Energy, and more, each contributing less than 3% of the total respondents.

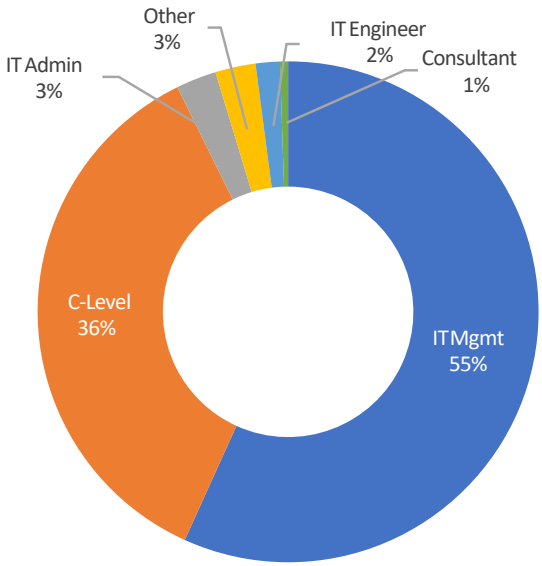


% of participating organisations by industry vertical

Respondents provided us with a broad representation of organisations of every sise, 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 year's report found a common theme of UK organisations confident in their security and yet expressed concerns reflecting a slightly less-shiny state of security. On average, **48% of organisations were concerned to some degree** about a security issue we raised.

Below are a list of the top issues keeping organisations "up at night":

- The top reason UK organisations are "up at night" is because of untrained and malicious users, **increasing concerns over cyber attacks an average of 125%**.
- **Insider Threat Detection and Credential Compromise** concerns were second and third biggest reasons organisations are "up at night".
- Shadow Apps and Devices top the list of attack types, with **75%** of UK organisations expressing some degree of concern.
- Ten different types of **cyber attacks** have an average of **68%** of UK organisations worried.
- Ensuring security is in place that meets **Compliance** requirements is still a challenge for **48%** of organisations, despite the regulation details being out for quite some time.
- **Adequate Budget** appears to remain a challenge for **63%** of organisations, impacting proper IT staffing, implementing solutions, and maintaining relationships with key vendors.

HOW MATURE IS THE UK'S SECURITY STANCE?

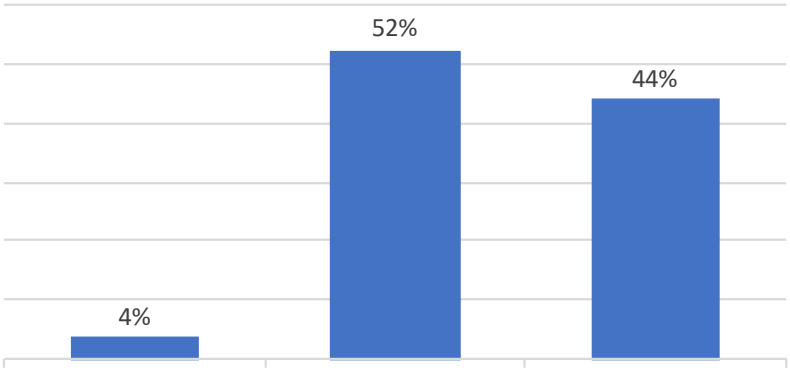
We started by asking our respondents about how they'd categorise their security strategy and organisational security culture. These high-level insights provide us with context around how organisations see their security stance.

Security Strategy

As shown below, we found an overwhelming majority of organisations believe they have either a *proactive* or *mature* security strategy in place.

We found the largest segments of both *proactive* and *mature* security strategies surprisingly in organisations with 50-100 employees, while a minimum of 43% of organisations in all size categories cite a mature security strategy.

Automotive, Hotel, Oil/Gas/Mining were the top three industries citing reactive security strategies and a lack of maturity, while Telecom, Legal, and Healthcare appear to be leading the way as industries with *mature* security strategies in place.



Reactive– We have no overarching security strategy per se, but have security solutions in place and are addressing issues ad hoc.

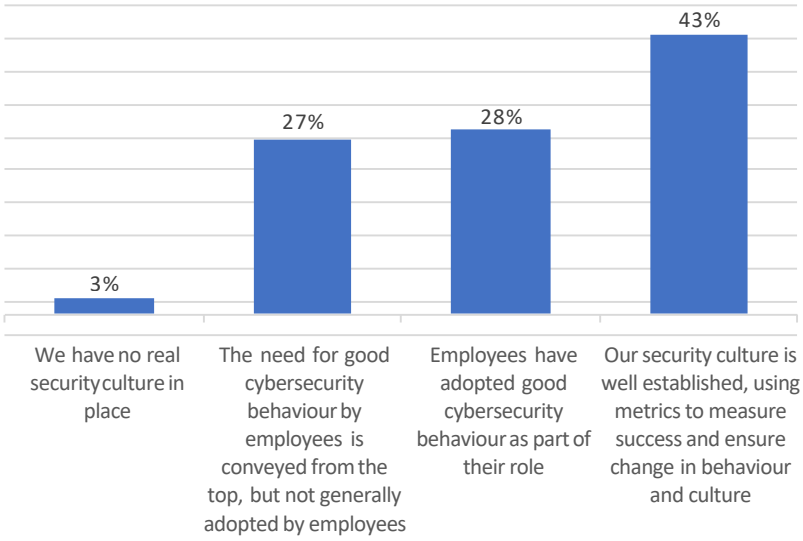
Proactive– We have purposely implemented solutions that will address both internal and external threats.

Mature– We have designed a well thought-out plan for a layered security strategy that addresses threats and risks we look to mitigate.

Security Culture

Because protection against and prevention of cyber attacks aren't simply a matter of how many security solutions you have in place, we also asked how each organisation would rank their security culture.

The need for employees to share the responsibility for protecting the organisation from data loss, data theft, malicious attacks, and fraud is critical to reducing the likelihood of a successful attack. A culture of security helps to establish and continually reinforce a state of employee vigilance.



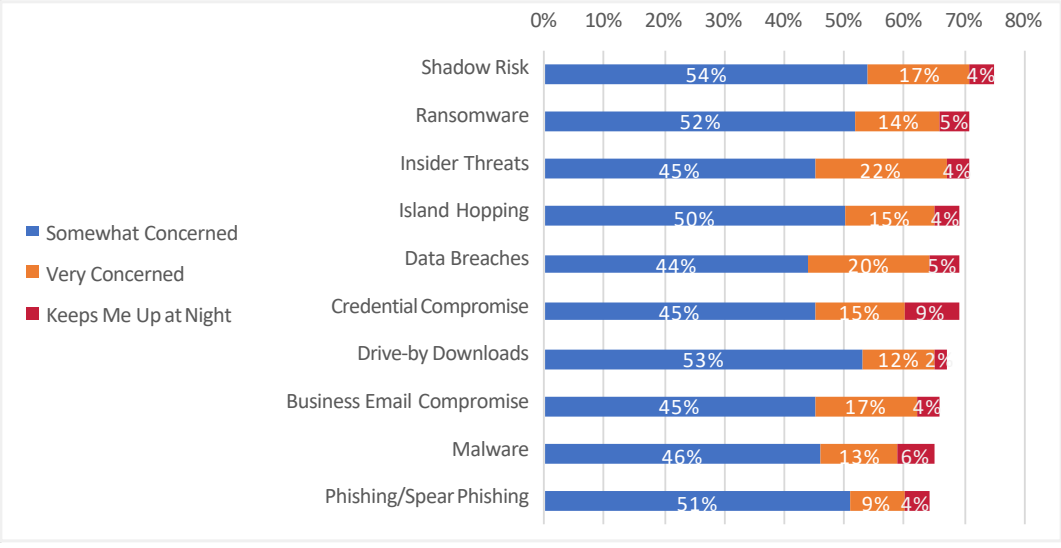
PRIMARY SECURITY CONCERNS

Concern #1: Attack Type

With the massive number of attacks organisations face on an annual basis, the work of preventing, monitoring for, detecting, alerting to, and remediating can become overwhelming. This causes organisations to often attempt to focus on just the most pressing attack vectors. So, which attacks are a concern? We broke the issue of attacks down into ten types:

- Business Email Compromise (Fraud)
- Credential Compromise
- Data Breaches
- Drive-By Downloads
- Insider Threats
- Island Hopping
- Malware
- Phishing / Spear Phishing
- Ransomware
- "Shadow" Risk/Unmanaged Assets

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



Of the ten attack types, every one of them has at least 64% of organisations concerned to some degree. The risk associated with "shadow" risk—a new category to this year's report, which generally includes unmanaged devices and applications—was the primary issue most organisations are concerned about. Return attack type, Ransomware, came in a close second, and newcomer Insider Threats appropriately jumped in as a top attack concern.

Credential compromise remains the top attack type keeping UK organisations up at night as cyber criminals go on the offensive. They are taking advantage of a pandemic-based remote workforce leveraging cloud applications that are seen as easy prey, needing only a basic phishing scam to trick users into giving up cloud credentials.

Concern #2: Compliance Security

Nearly all compliance regulations today include some degree of prescriptive data security mandates; the risk of data breaches involving personally identifiable information and the threat of compliance fines are enough to get the attention of IT. So, which regulations do organisations have a grasp on, and which ones are still not completely secure and compliant? We focused on six of the most pressing compliance and best practice standards—some very much originating in the United States, some industry-specific, and some laser focused on protecting consumer data:

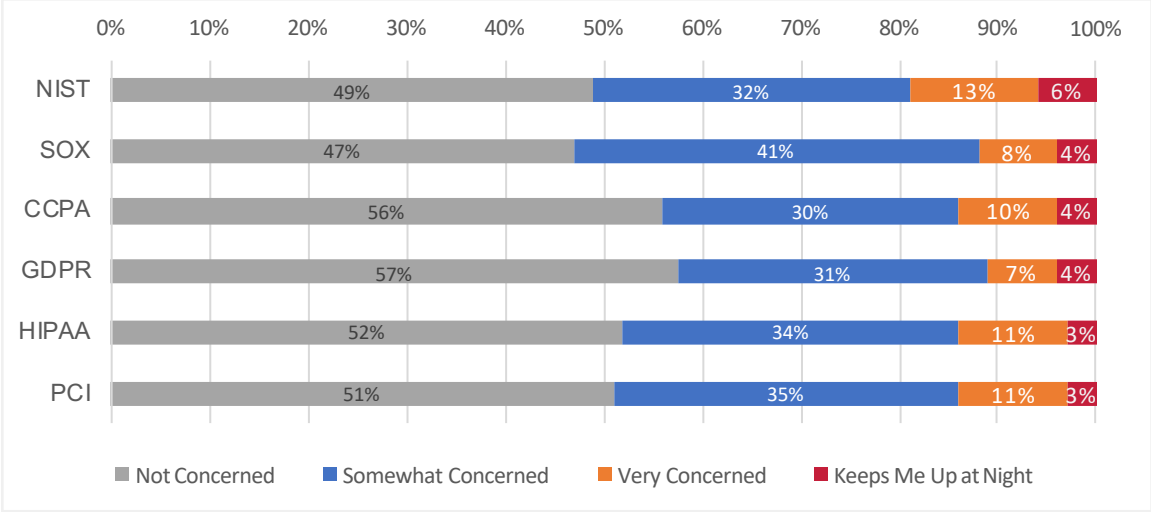
- GDPR
- HIPAA
- CCPA
- PCI
- SOX
- NIST

On the average, 84% of UK organisations cited being subject to these regulations.

To provide more color, the answers we provided were:

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

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

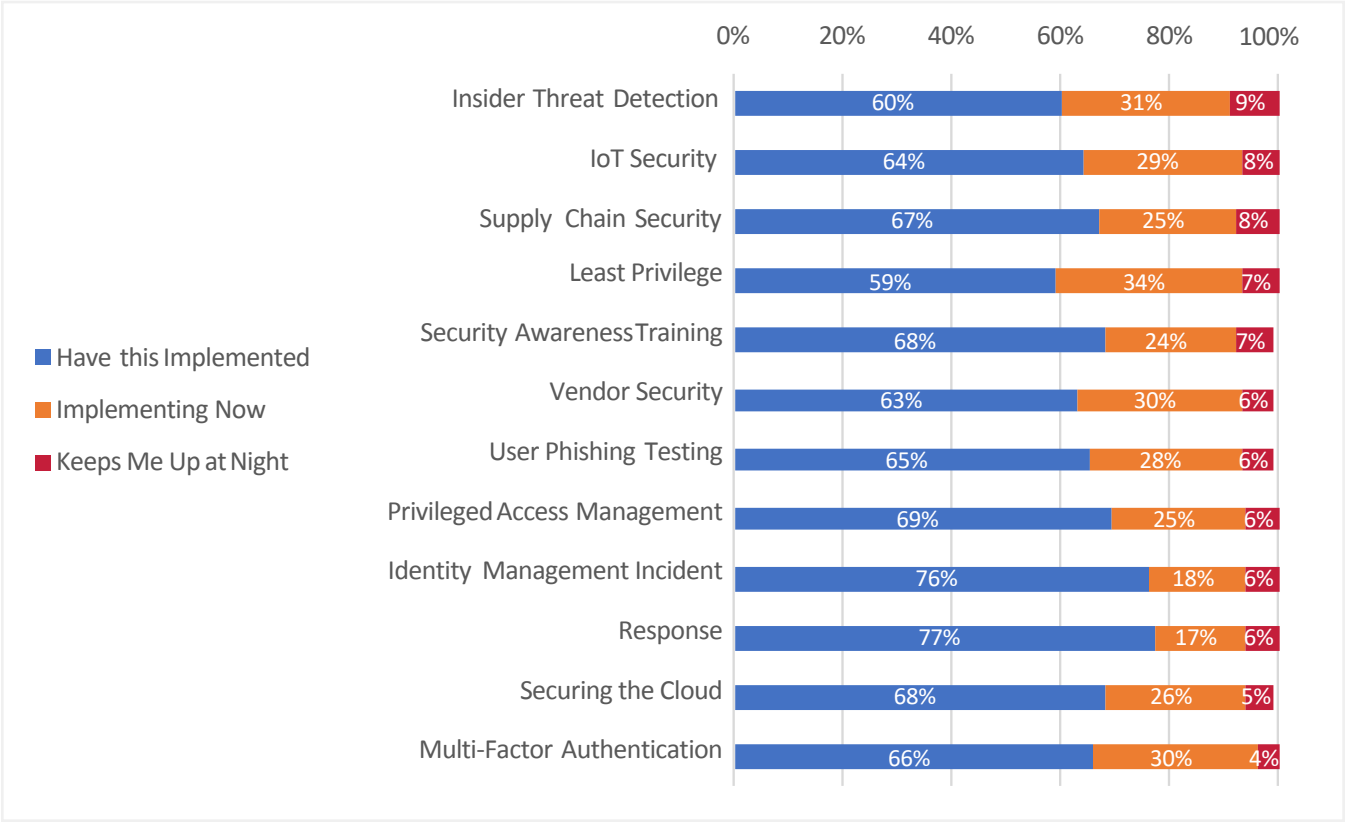


Surprisingly, ensuring security related to U.S. regulations HIPAA and SOX that have both been around for decades appears to be as much an issue for UK organisations as newer regulations, such as GDPR. We're somewhat glad to see NIST security standards topping the list with the highest levels of concern, as it indicates, organisations are embracing these best practices to strengthen their security.

Concern #3: Security Initiatives

The key to any proper defence against cyber attacks is a layered security strategy. With it, you have a better chance of identifying risks, proactively strengthening your human defences, detecting threats, and remediating attacks. There are lots of security initiatives that can play a role in a layered security strategy, but not every organisation has every single one of them implemented. So, which security initiatives have been addressed and which are still an issue?

We asked about twelve common initiatives that play a role in a layered security strategy. The chart below shows the level of concern around implementation of each security initiative for those organisations indicating they do not have a current implementation in production.

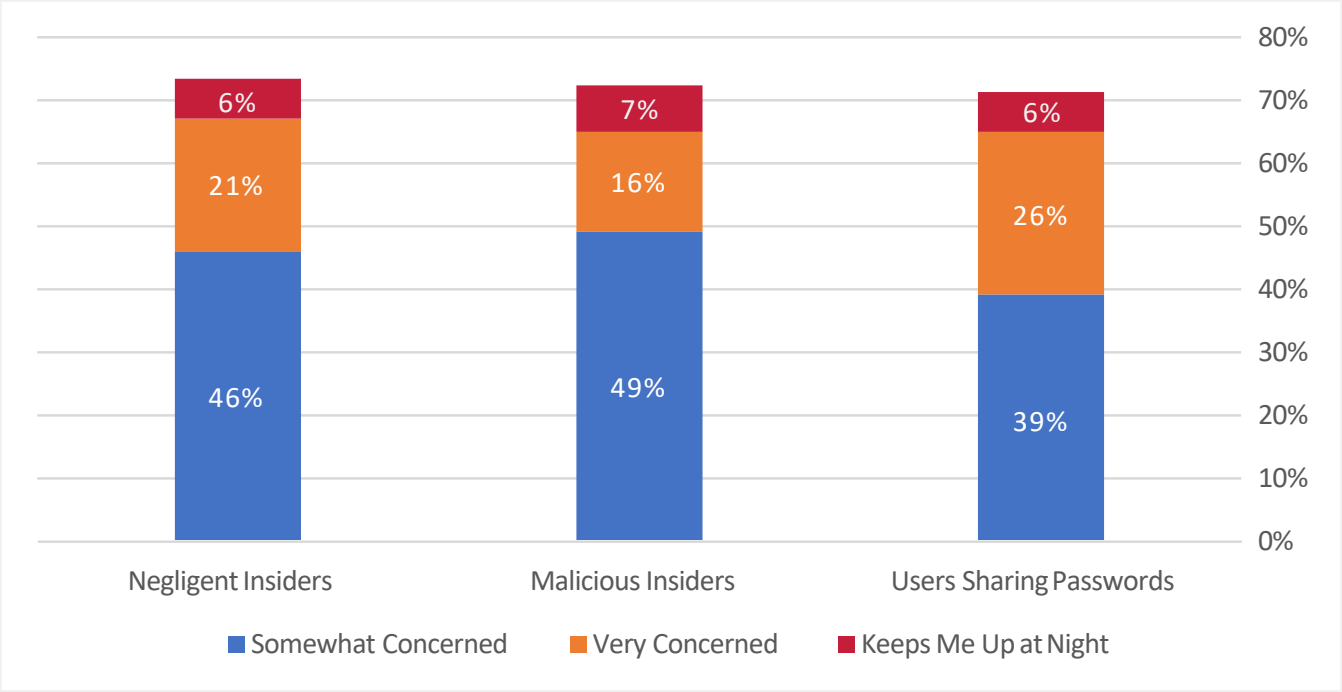


Detecting Insider Threats topped our list of security initiatives keeping UK organisations "up at night". Insider Threats ranked third in our previous list of attack concerns, so it's no surprise to see detection solutions as the initiative most keeping you up at night. It's refreshing to see both IoT and Supply Chain security as concerns, demonstrating that UK organisations are thinking about their security stance well outside the normal perimeter of devices and users.

On average, 10% of organisations stated a given security initiative did not apply to them. Of those implementing these security initiatives, UK organisations have an average of just under eight solutions completely implemented, with very little differentiation in that count based on organisation size.

Concern #4: Users

Nearly every initial attack vector—such as emails, links, attachments, webpages, and more—requires the interaction of a user, making the user the pivotal point between a successful attack or defence. So, we wanted to understand on which side of the equation do UK organisations see their users.



The *negligent user* was the second greatest "up at night" concern in this report, sitting just behind a tie between detecting insider threats, and the use of shadow applications and devices. This concern around the negligent insider is well-founded: in digging deeper into the data, we found that the negligent user *is the single greatest factor in determining "up at night" levels of concern*. For example, when looking at the breakout of organisations citing "up at night" concern for each attack type mentioned previously in this report, the percentage of organisations very concerned *jumps by an average of 125%* when you factor in only those organisations that are up at night about negligent users. The concern of data breach jumps *260%* in those organisations also concerned about the negligent insider.

In essence, those organisations worried about negligent users are far more worried about cyber attacks.

Malicious insiders are responsible for 23% of insider incidents[1], so it's no surprise we see this as a close second place concern. We also see users sharing passwords is not far behind in overall concern, but achieves nearly the same level of "up at night" concern as the negligent user. Similar to the negligent user, those organisations "up at night" over compromised credentials are three times more concerned over users sharing passwords than the average organisation.

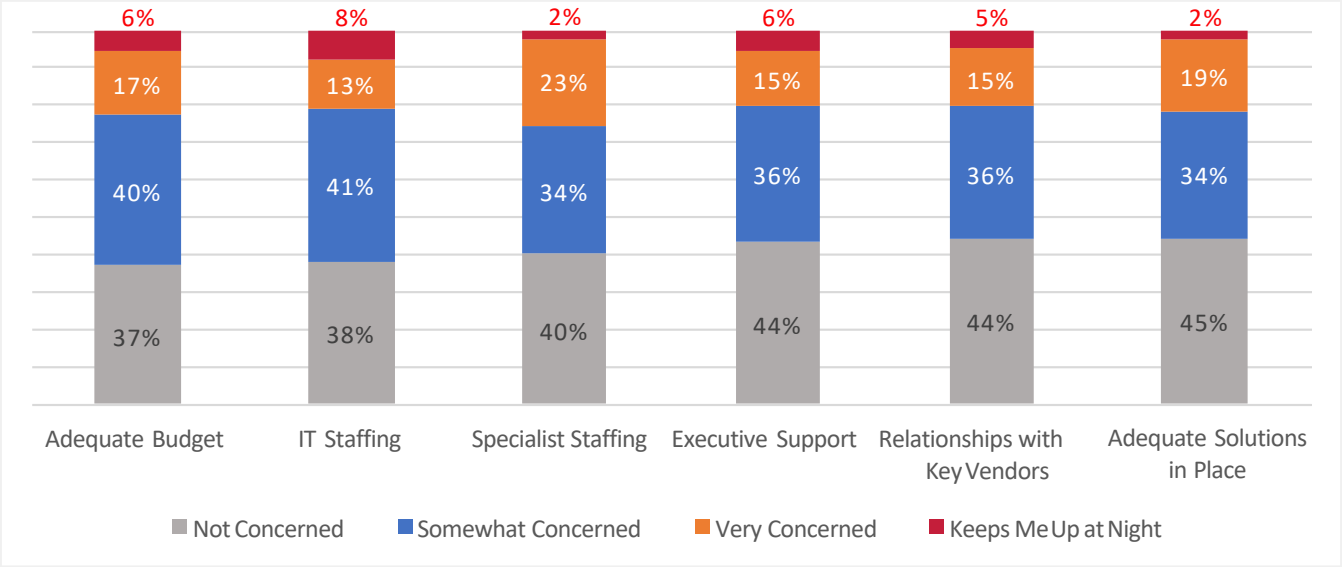
Of those organisations previously citing having a *mature* security strategy, 71% are *still* concerned about negligent users, 69% are concerned about malicious insiders, and 71% are concerned about user's sharing passwords. In short, *the user remains a material concern*.

1 Ponemon, *Cost of Insider Threats Global Report* (2020)

Concern #5: Resources

A common source of IT's inability to properly secure the environment can revolve around a lack of resources. Nearly every concern we've raised so far in this report can easily be attributed back to a deficiency in one or more resources—whether it be budget, staffing, internal expertise, executive support, relationships with vendors, or having the right solutions.

So, we wanted to understand where IT organisations lacked the proper resources. We focused on five common issues plaguing IT. The chart below shows the majority of organisations have issues across the board, with the greatest overall resulting challenge as putting proper solutions in place.



Budget remains the top overall concern for most IT organisations. Of those organisations citing a concern over adequate budget, the average organisation had only six of the thirteen security initiatives in place (as compared to the overall average of eight initiatives) and elevated levels of concern across nearly all of the areas covered in this report. IT staffing issues come in second place as an overall concern, but tops the resource list keeping you "up at night". The source of this issue may actually be related to budget, as those organisations citing staffing concerns have an 80% overlap with those organisations having budget issues. Additionally, those "up at night" over staffing have an average of only five security initiatives implemented—all indicators pointing to budget as the culprit.

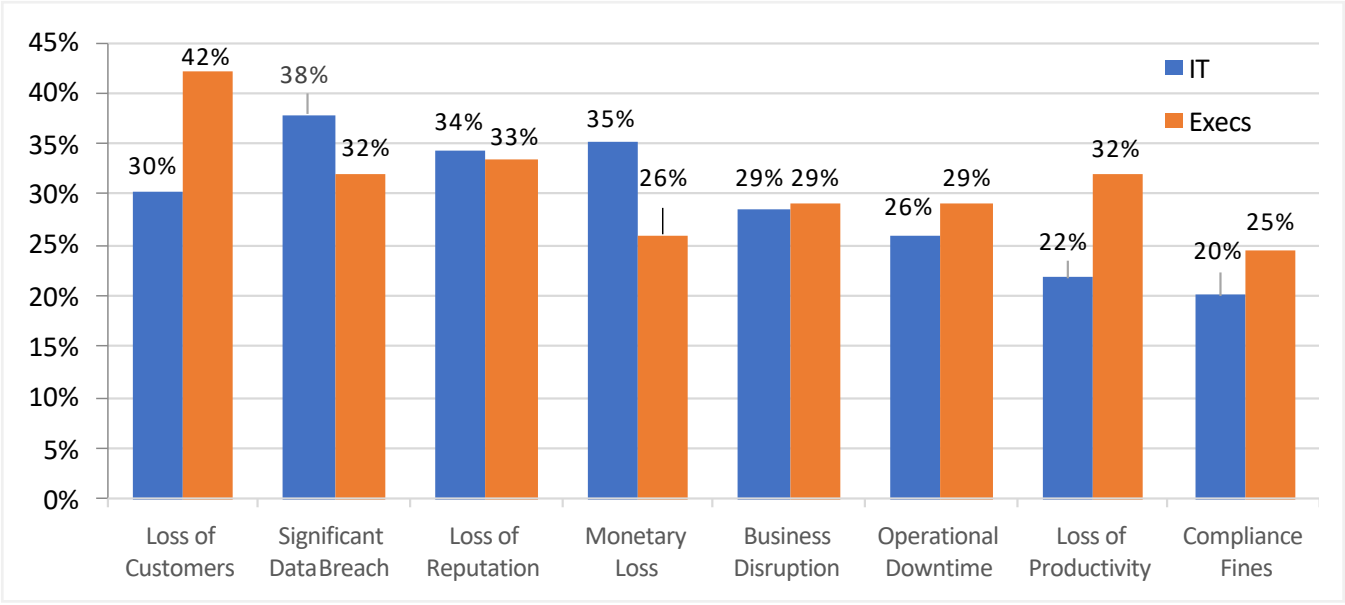
Executive support seems of less concern, although it ties for second place as an "up at night" concern, tied with budget, as another factor impacting budgets and, with 77% overlap between organisations concerned with inadequate budget and those concerned about executive support.

And while having adequate solutions was near the bottom of our resource concern list, the organisations citing both being "very concerned" and "up at night" about not having adequate solutions jointly outweigh the corresponding combined values in each of executive support and having key vendors.

Concern #6: Executive Issues

The C-Suite of UK organisations is far more concerned with strategic initiatives and any business disruption that may keep those initiatives from succeeding. IT generally concerns itself with a far more tactical perspective around keeping the business running. We asked both executives and IT which business issues are of concern to the executive level of their organisation.

The data shown below breaks out the responses by those indicating their role in the organisation as an executive and those indicating an IT position. As shown, by and large, the IT staff concerns are misaligned with that of their executive team.



The loss of customers topping the executive's list is odd, given it represents the result of many of the operational threats listed in this chart. IT has their eye first and foremost on data breaches, but does seem to be very aware of the business outcomes from data breaches and other business disruption.

GETTING A GOOD NIGHT'S REST

The state of IT's concerns reflects their true state of security. Regardless of whether you believe your security to be well-established and functioning well, the presence of concerns helps indicate whether the strategy is either flawed or not well executed. Based on the report findings, many of your organisations are all experiencing the same challenges in execution. The problem may simply be a disconnect between the technology needed and executive focus. 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 and Execute a Security Strategy**—An average of 33% of you are "working" on security initiatives or need to get started, and 56% of you don't yet have a mature security strategy in place. And, for those of you who believe you do have a mature security strategy, consider the possibility that there is a disconnect between the strategy and the execution—particularly in the way of educating and requiring users to use secure best practices. The data around concerns provides context as to whether the strategy is being implemented correctly.

2 **Get Executive Buy-In**—56% 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 organisation should security not be made a priority.

3 **Obtain Necessary Budget**—63% of you don't have the budget necessary. Using your plan, prioritise 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 users. 75% of you are worried about the risk of shadow applications and devices, and 73% of you are concerned with negligent users. Users need to first understand their role in organisational security, and then learn to stop entertaining phishing scams, clicking on links, providing credentials to fake websites, and using shadow IT. It starts with establishing a security culture. Remember, there was a **125% increase in "up all night" concern for cyber attacks** in organisations with major concerns around 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 inboxes, you're still at risk. Implement security awareness training and simulated 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 defence and lower organisational risk.

57% of organisations indicated they had security awareness training implemented. But, given the level of concern around negligent users, sharing of passwords, and cyber attack methods that require the engagement by a user to be successful, it's likely that your training is little more than breakroom training that is forgotten once users leave the room.

Additional Resources

About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realising that the human element of security was being seriously neglected, KnowBe4 was created to help organisations manage the ongoing 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 mobilise their end users as a last line of defence and enable them to make smarter 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
KnowBe4 UK, Ltd. | Osprey and Kestrel, The Hawkhills Estate, Easingwold, York YO61 3FE | +44 (0) 1347 487512

V061120