KnowBe4
Human error. Conquered.

WHITEPAPER

The 2020 What Keeps You up at Night Report

Benelux Edition

Table of Contents

ABOUT THIS REPORT

Today, maintaining organizational security against cyberthreats is a unique challenge of trying to hit an always-moving target with a toolset that is trying to keep up. Cybercriminals are focused on the targeted game, identifying specific industry verticals, organizations, and even individuals, and maximizing success by devising tailored scams and attacks. In addition, we are seeing increases in frequency, sophistication, and scope of ransomware, phishing, business email compromise, and malware-less attacks.

We are also watching cyberattacks evolve. To increase the chances of successful attacks, ransomware has grown to include data theft and extortion. Attackers are not using deepfake audio to trick users over the phone, and they are no longer satisfied with raking in thousands of dollars when millions are plausible.

In response, IT organizations have been tasked with trying to establish and maintain a layered security strategy that protects the organization and its users, preventing ever-changing threats from gaining a foothold within your organization. Much of the constant barrage of threats, attacks, malware, and news stories must have some IT organizations deeply worried.

So, we wanted to find out what has changed since we initially published this report last year. While the 2019 report covered the globe, this year's results are broken into geography-specific reports. In this report, we're seeking to understand which issues are keeping Benelux organizations "up at night," that is, which aspects of security—from attacks, to security initiatives, to risks, to organizational constraints—are you most concerned about.

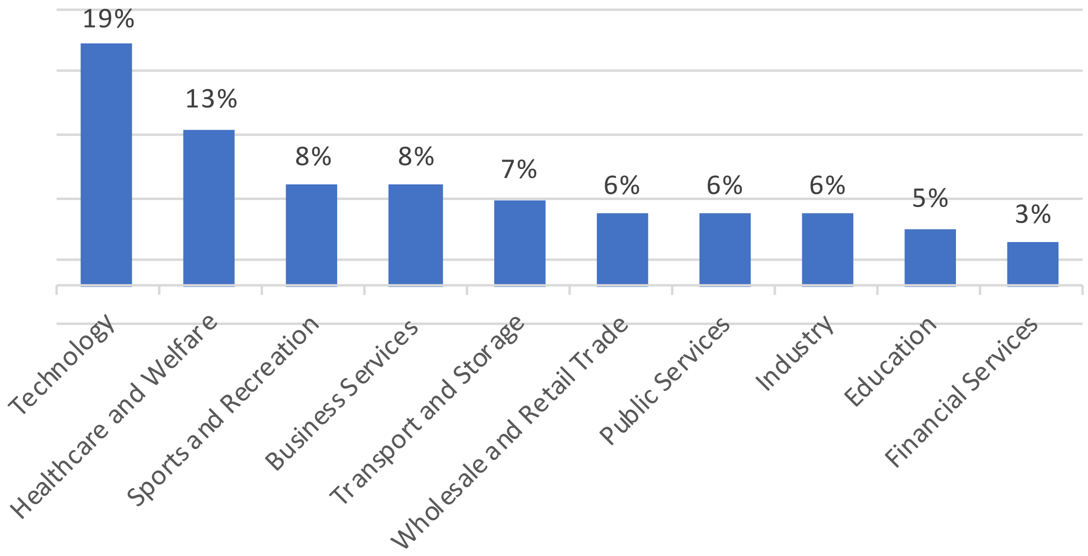
In this report, we are going to look at the state of security from six perspectives:

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

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

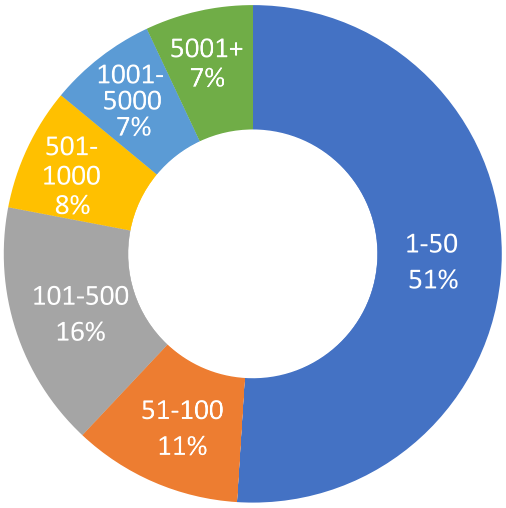
ABOUT OUR RESPONDENTS

Nearly 100 organizations across Benelux participated in this year's report. The top 10 industry verticals represented in this report are shown below. The other industries included Agriculture, Utilities, Construction, Real Estate, and more, each contributing less than 3% of the total respondents.

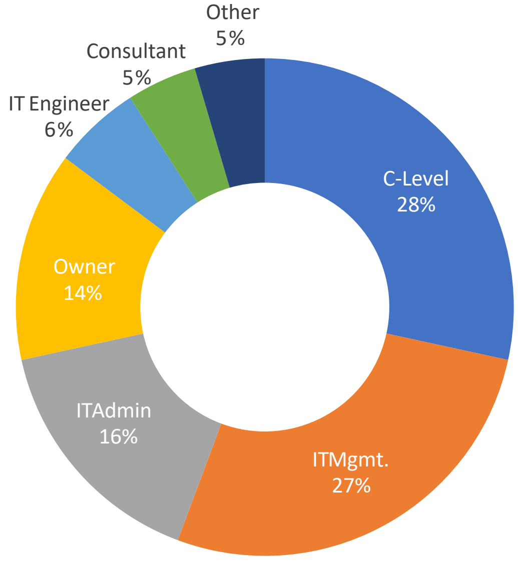


% of participating organizations by industry vertical

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 year's report found a common theme of Benelux organizations confident in their security, but also of concerns reflecting a slightly less-shiny state of security. On average, **58% of organizations were concerned to some degree** about a security issue we raised.

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

- Concern for **Credential Compromise** was the number-one concern across the report keeping the most organizations "up at night."
- **Ransomware** topped the list of attack types causing the greatest over all concern, with **78%** of organizations expressing some degree of concern.
- **Negligent Users** were the top user concern this year for **68%** of organizations, resulting in **70%** of organizations being concerned about cyberattacks needing user involvement to succeed.
- Ten different types of **cyber attacks** have an average of **65%** of Benelux organizations worried.
- **Implementing Security Initiatives** remains a challenge for 82% of organizations who are still working on putting needed parts of their layered security strategy in place.
- **Adequate Budget** appears to remain the number-one resource challenge for organizations, impacting proper security specialist staffing and implementing solutions.

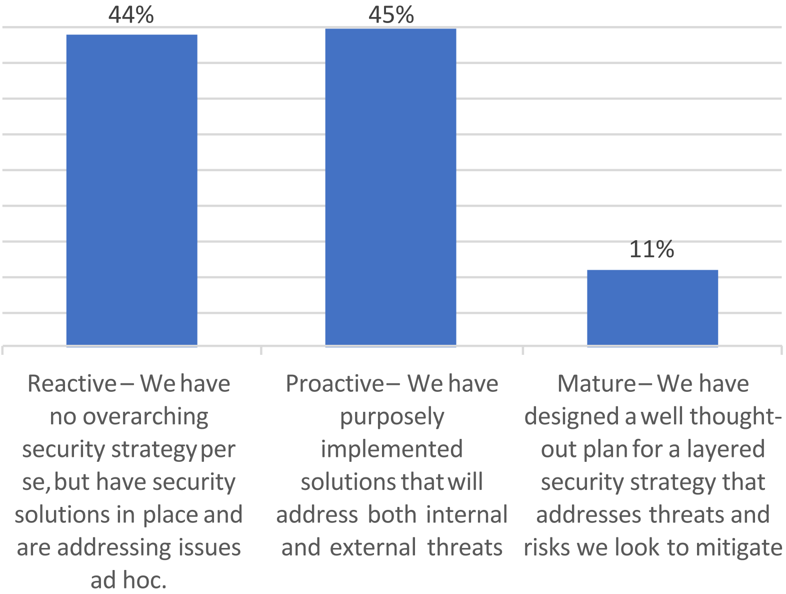
HOW MATURE IS THE BENELUX SECURITY STANCE?

We started by asking our respondents about how they would categorize their security strategy and organizational security culture. These high-level insights provide us with context around how organizations see their security stance.

Security Strategy

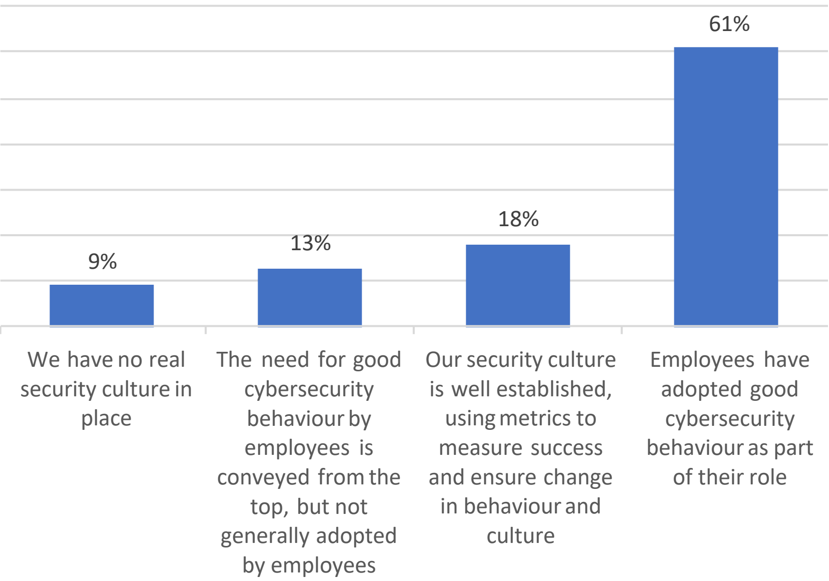
As shown below, we found most organizations split between *reactive* and *proactive*.

All small and medium businesses (those with less than 500 employees) seem to be acting reactively, as all organizations above 500 employees cited either a *proactive* or *mature* security strategy. As you will see in this year's report, there appears to be a disconnect between an appropriate level of concern around every aspect of security we ask about and the organizations own perceived level of security maturity. We'd expect to see very high degrees of concern but find that only a moderate level of concern exists across the Benelux organizations.



Security Culture

Employees need to share the responsibility of protecting the organization from data loss, data theft, malicious attacks, and fraud. The assumption of a state of security culture seems to somehow carry across organizations, despite the high percentage of those with a reactive security strategy. The remainder of this report somewhat demonstrates that the opposite is true.



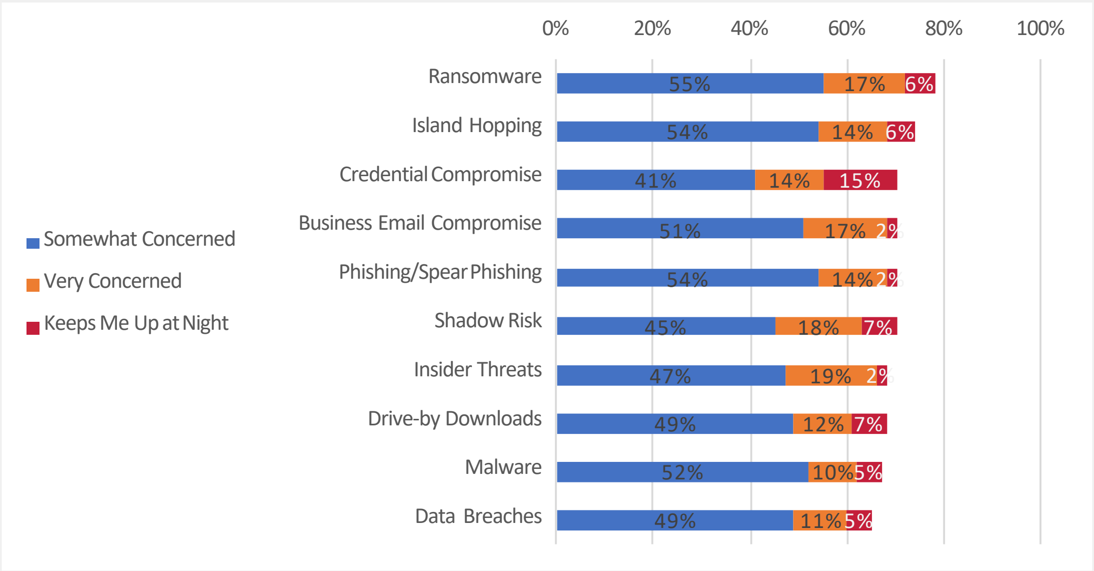
PRIMARY SECURITY CONCERNS

Concern #1: Attack Type

With the massive number of attacks organizations face each year, the work of preventing, monitoring for, detecting, alerting to, and remediating can become overwhelming. This often causes organizations to attempt to focus on just the most pressing attack vectors. So, which attacks are a concern? We broke down the issue of attacks into 10 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 organizations.



Of the 10 attack types, every one of them has at least 65% of organizations concerned to some degree. The risk associated with credential compromise—which generally is the result of successful phishing and/or social engineering attacks—was the primary issue most organizations are concerned about. It is interesting to see this as an absolute concern outlier, given that 43% of the organizations "up at night" over this issue cited having a "mature security strategy" and a little over one-quarter cited having a "well-established" security culture.

Ransomware attacks are given the most total concern by Benelux organizations. This is well-founded, as cybercriminals are going on the offensive, taking advantage of a pandemic-based remote workforce, and leveraging internal credentials and known system and application vulnerabilities to infect organizations with ransomware while also adding data exfiltration as a tactic to ensure ransoms are paid.

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 organizations have a grasp on, and which ones are still not completely secure and compliant? We focused on seven of the most pressing compliance standards and best practices—some originating in the United States, some EU-based, some industry-specific, and some laser focused on protecting consumer data:

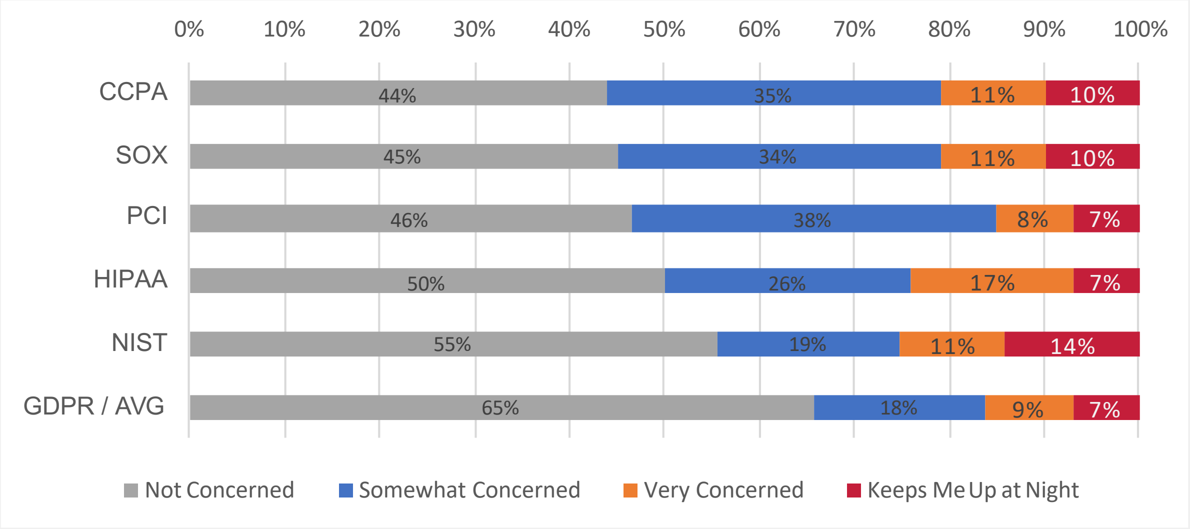
- GDPR / AVG
- HIPAA
- CCPA
- PCI
- SOX
- NIST

On average, 75% of Benelux organizations 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 on-going 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 organizations *that indicated they are subject to each compliance mandate*.

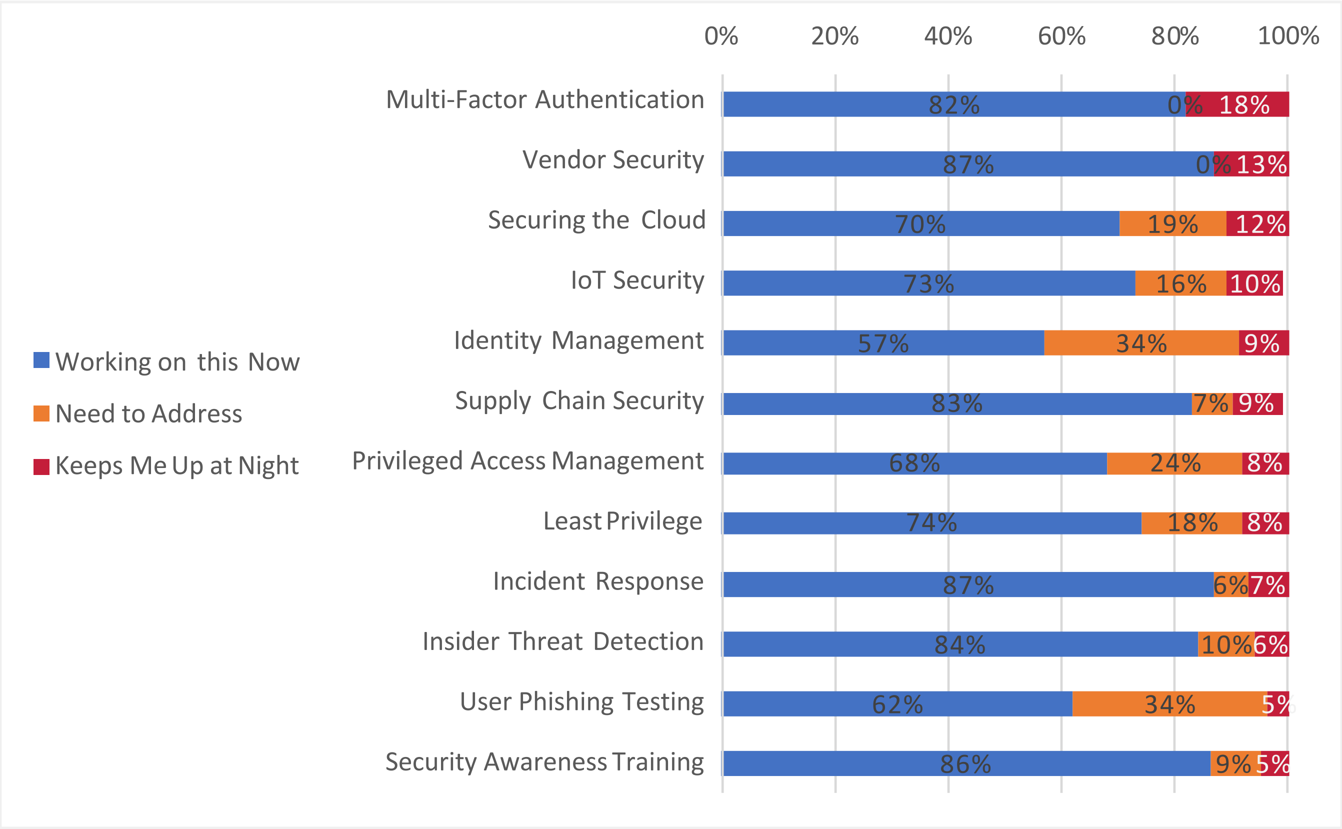


We are glad to see nearly two-thirds of organizations ready for GDPR/AVG, and over half embracing NIST best practices for keeping the environment secure. Surprisingly, organizations still do not have a handle on their security related to U.S. regulations HIPAA and SOX that have been around for decades. CCPA and PCI are also of concern, with over half of organizations still working on getting their security compliant.

Concern #3: Security Initiatives

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

We asked about 12 common initiatives that play a role in a layered security strategy. On average, 18% of organizations stated a given security initiative did not apply to them. The chart below shows the level of concern around implementation of each security initiative for those organizations indicating they do not have a current implementation in production.



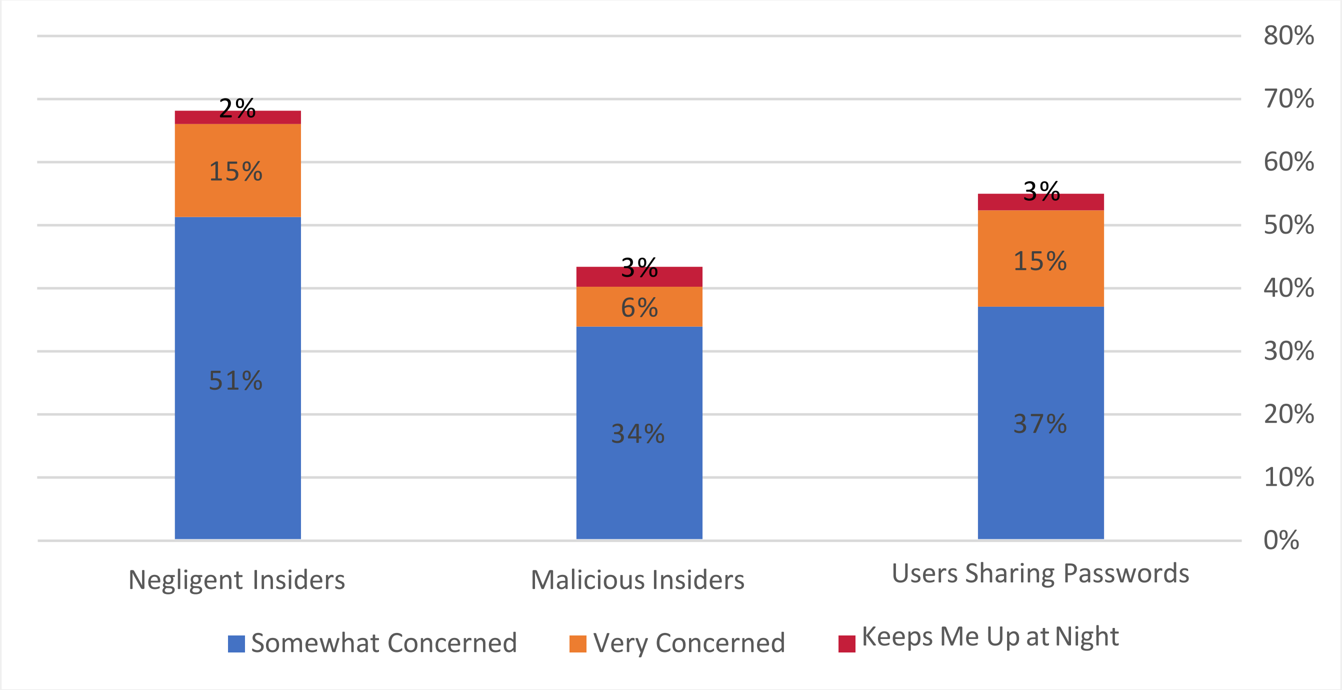
Multi-Factor Authentication topped our list of security initiatives keeping Benelux organizations "up at night"—this aligns with the overarching concern around compromised credentials. Identity management (another aspect of shoring up credential security) showed the lowest percentage of organizations currently working on the initiative. These two pieces of data may shed some light on why credential compromise is such a great concern to organizations. Organizations simply are not ready.

Of those implementing these security initiatives, organizations have an average of just over four solutions completely implemented. Those organizations with a mature security strategy averaged just under nine solutions, while those citing "good" or "well-established" security cultures averaged just under three solutions implemented.

But, it's the use of a layered security strategy—that involves using multiple types of solutions at various parts of attack—that provides the greatest levels of protection.

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 defense. So, we wanted to better understand on which side of the equation do Benelux organizations see their users.



Negligent insiders spawned the greatest overall user concern in organizations. While very few organizations consider themselves "up at night" over users unwittingly participating in attacks, the overall level of concern aligns with organizations' concerns over the various types of cyberattacks, and most of which rely on a negligent user's participation to be successful.

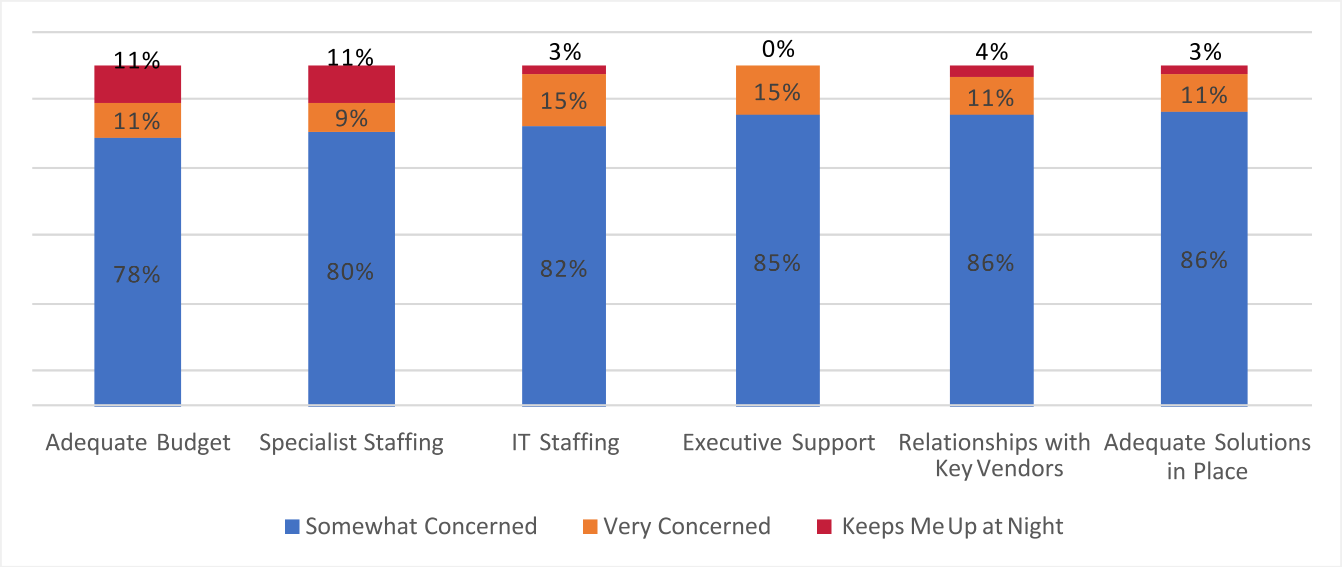
While malicious insiders are responsible for 23% of insider-related incidents[1] , we are surprised to see such a low degree of concern for the malicious user. And the low overall concern for users sharing passwords and malicious insiders does not align with the high degree of concern seen previously for compromised credentials.

[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 have raised so far in this report can easily be attributed 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 organizations lacked the proper resources. We focused on six common issues traditionally plaguing IT. The chart below shows many organizations have issues across the board.



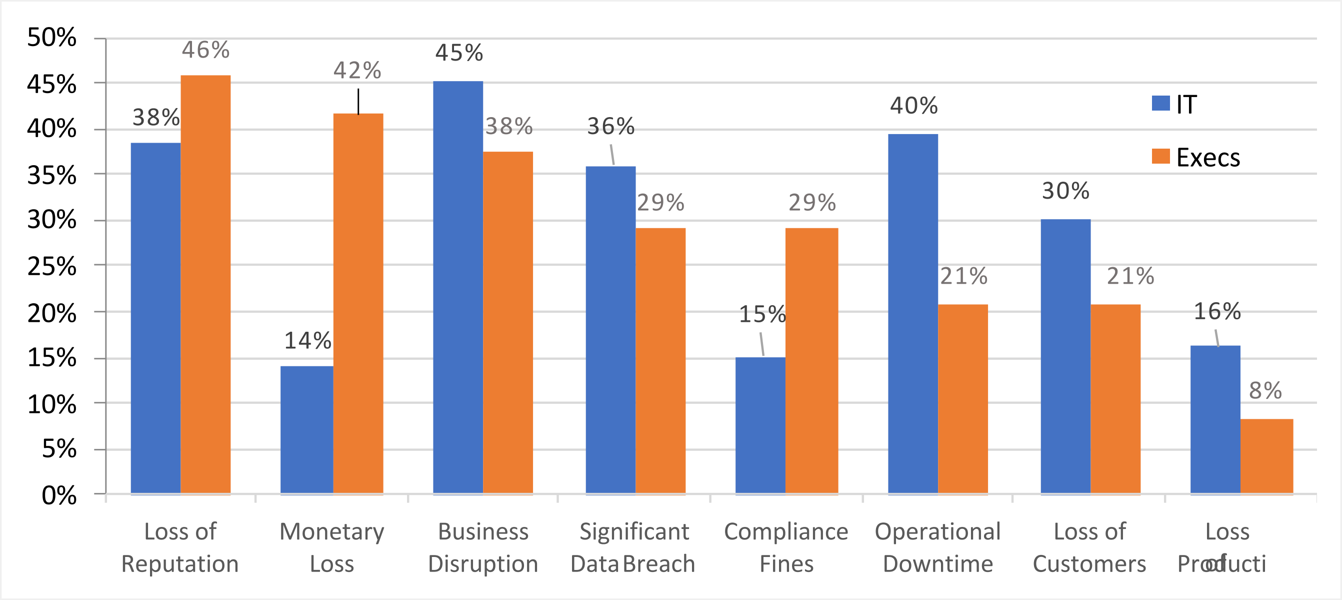
On average, just under 64% of organizations cited having no concerns for any of the resource issues raised here. Of those that did express concern, shown above, budget remains the top overall concern for most IT organizations, with the largest percentage of organizations either very concerned or "up at night." Of those citing concern over adequate budget, the average organization had only implemented three of the 12 security initiatives previously mentioned, and experience elevated levels of concern across nearly all the areas covered in this report. Security specialist staffing issues come in second place as an overall concern but shares the first-place spot for keeping organizations "up at night." The source of this issue may be related to budget, as those organizations citing staffing concerns have a 75% overlap with those organizations having budget issues. Additionally, those "up at night" over security specialist staffing have an average of only three security initiatives implemented—all indicators pointing to budget being the culprit.

Executive support seems of less concern, with no organizations kept "up at night" over this issue, but with 15% of organizations remaining very concerned. Despite this, the impact of having not enough executive support was clear in the data: just under two of the 12 security initiatives were implemented, 75% of these organizations were "up at night" over not enough security specialists, and half of them cited their security strategy as being "reactive" in nature.

Concern #6: Executive Issues

The C-Suite of Benelux organizations 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 organization.

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



Loss of Reputation, Monetary Loss, and Business Disruption were at the top of the executives' list, while only two of the three were of greatest concern to IT teams. IT substitutes operational downtime as one of their top three concerns but does seem to be very aware of the business outcomes from this downtime and its impacts, based on their alignment with at least two of the three top executive concerns.

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 where in the strategy is either flawed or not well executed. Based on the report findings, many of your organizations are all experiencing the same challenges in execution and an interesting, distinct lack of concern when compared to the rest of the world. The problem may simply be a disconnect between the technology needed and executive focus. 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**—A massive 82% of you are "working" on security initiatives or need to get started, while 75% of you do not yet have a mature security strategy in place. And, for those of you believing 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**—Twenty six percent of you do not have enough support. Educate your executive suite on the security challenges you are 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**—Thirty six percent of you do not have the budget necessary. Using your plan, prioritize what is 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. Despite 61% of you citing a culture where the user has adopted good cybersecurity behaviors, a minimum of 65% of you are worried about cyberattack types that each require the involvement of users, and 68% of you are concerned with negligent users. This demonstrates that IT does not truly understand what a real organization-wide security culture entails. Users need to first understand their role in organizational security, and then learn to stop entertaining phishing scams, clicking on links, providing credentials to fake websites, and using shadow IT. Establishing a security culture starts with proper user Security Awareness Training. Eighty two percent of organizations indicated they are working on implementing Security Awareness Training. But, given the level of concern around credential compromise, negligent users, and cyberattack methods that require the engagement by a user to be successful, it is likely that your training is little more than breakroom training that is forgotten once users leave the room.

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 customised 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. Realising that the human element of security was being seriously neglected, KnowBe4 was created to help organizations 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 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 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.de

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 NL | Papendorpseweg 99, 3528 BJ Utrecht, Netherlands | +31 (30) 7996074

V082120