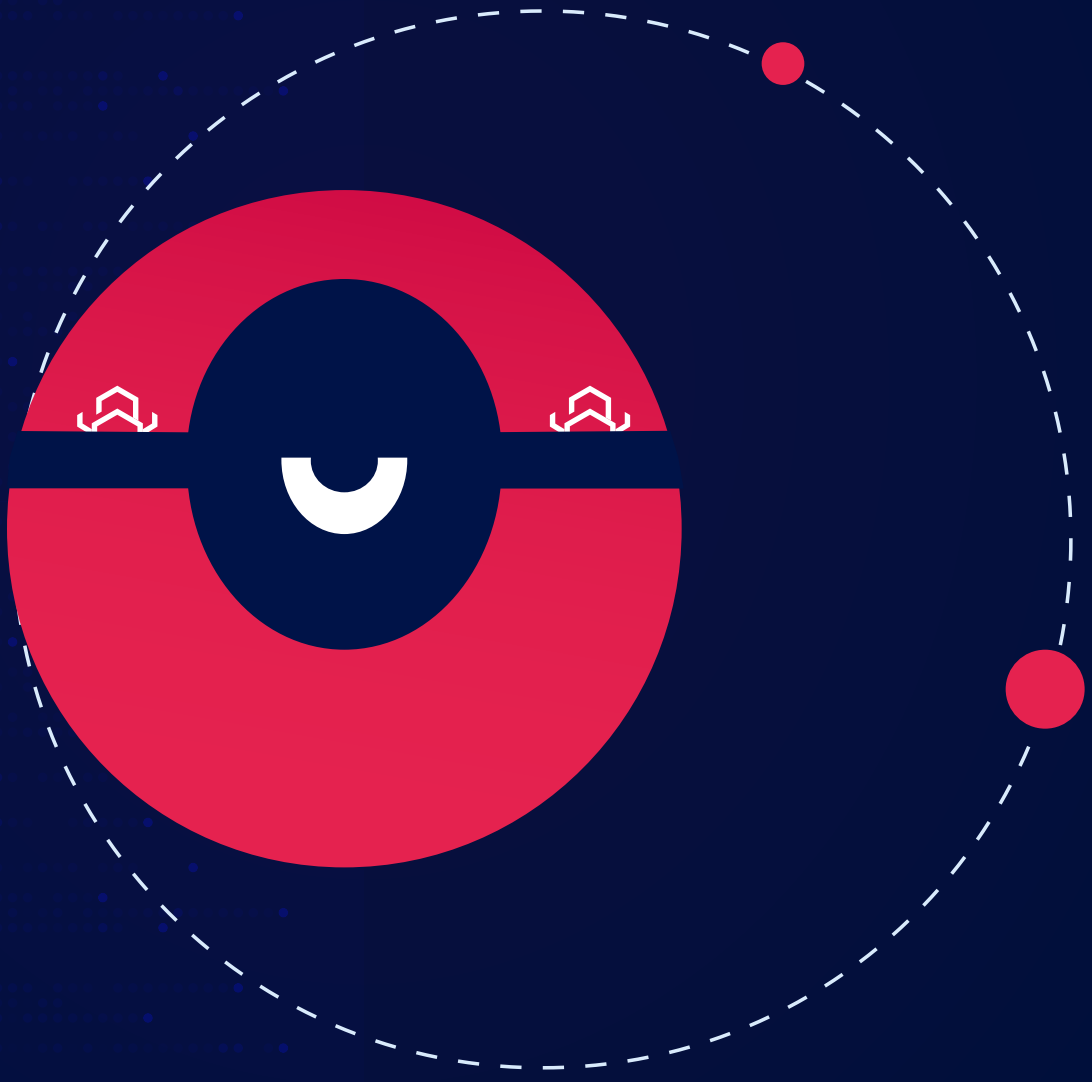
netwrix

2020 CYBER THREATS REPORT



www.netwrix.com

EXECUTIVE SUMMARY

When the 2020 pandemic hit organizations around the world, many of them scrambled to enable their employees to work from home. Almost immediately, news outlets were reporting a skyrocketing number of cyberattacks on the newly broadened IT infrastructures, as well as targeted attacks on employees trying to adjust to their new work-from-home environment.

In June 2020, we surveyed 937 IT professionals from all over the globe to learn how their threat landscape and priorities have changed due to this massive shift to remote work. The findings, which are presented here, will help organizations re-assess their security risks and identify new security gaps.

Significant findings include:

- 39% of respondents said they tightened their data security during the pandemic, but 24% reported that their organization is at greater cybersecurity risk than before.
- 63% reported an increase in the frequency of cyberattacks.
- 60% found new security gaps as a result of the transition to remote work.
- 58% reported employees ignoring cybersecurity policies and guidelines.

But the most troubling finding in this survey is that 85% of CISOs said that they sacrificed cybersecurity to enable employees to work remotely. And that's just those who admitted it.

Nearly half (48%) of the organizations surveyed reported phishing attacks during the first three months of the pandemic; 86% of them were able to detect the attack in minutes or hours. Other common threat patterns included accidental misconfigurations by IT admins (27%) and improper data sharing (26%); both of these types of incidents were discovered in days or weeks by 48% of organizations. Every fourth organization reported experiencing a ransomware or other malware attack.

Diving down one level into the types of cyber threats that are keeping IT pros up at night, the survey found the following:

- 85% are concerned about VPN exploitation — an increase of 59 percentage points from pre-pandemic.
- 66% are worried about cloud misconfiguration (an increase of 18 percentage points).
- 66% are anxious about the possibility of data theft by employees (increased by 12 percentage points).

What's interesting about these findings is that only the VPN vulnerability could be characterized as an external threat (one that can be leveraged by hackers); the other two are associated with internal actors, such as IT personnel and regular business users.

66% of the IT professionals surveyed regularly report to the executive leadership on the state of cybersecurity. They use the following metrics the most:

- Incident statistics (61%)
- Vulnerability statistics (57%)
- General "state of cybersecurity" score (56%)

Financial metrics, such as total cost of ownership and return on investment, were listed by less than a quarter of respondents. For many, reporting takes up a fair amount of time: 41% of respondents claimed that they or their colleagues are spending more time and effort to generate reports than they should be.

CHAPTER 1

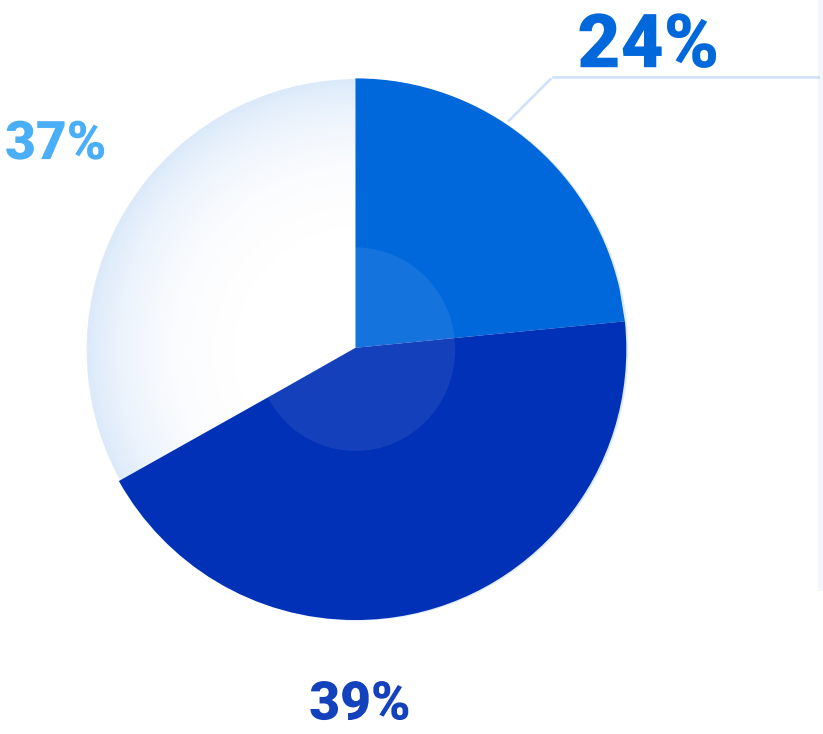
WFH Impact on the Threat Landscape

"Challenging" and "hectic" aren't strong enough words to describe rapid transition to remote work. Surprisingly, 39% of respondents believe that their security posture has actually improved during these uncertain times. Whether they strengthened old security policies or adopted new tools, we are very glad that some organizations were able to rise so quickly to the challenge presented by this crisis.

However, every fourth respondent said that their organization was more vulnerable to cyber threats than it had been before the pandemic. 63% of them said that cyberattacks were more advanced and/or more frequent than before. 60% are afraid that they may have left some security gaps when they were rapidly enabling employees to work remotely, while 58% are concerned that employees might ignore security rules and put data at risk.

Threat landscape change since transition to remote work

- We are at greater cybersecurity risk than before
- We increased our cybersecurity
- Nothing has changed



Stronger cyber attacks	63%
Unexpected security gaps	60%
Users may ignore security guidelines	58%
Sacrificed security in favor of availability	46%
Lack of visibility	36%

IMPACT ON ORGANIZATIONS BY SIZE

About half of small organizations (those with up to 100 employees) said that the pandemic didn't have any impact on their data security, and the other half were fairly evenly split between saying they are at greater risk and saying they have improved their cybersecurity. In contrast, about half of medium and large organizations claimed that the rapid transition to remote work actually helped them strengthen their security controls.

Most organizations, regardless of size, that say they are at greater risk cited increased intensity of cyberattacks and employee negligence in following corporate cybersecurity guidance.

*Threat landscape change by organization size**

	Small 1-100	Medium 101-1,000	Large 1,001+
We are at greater cybersecurity risk than before	21%	29%	23%
We have increased our cybersecurity	28%	43%	47%
Nothing has changed	51%	28%	30%

Small businesses are defined as organizations with fewer than 100 employees; medium enterprises are those organizations with 101 to 1,000 employees, large enterprises are those with more than 1,001 employees.

ADDITIONAL HIGHLIGHTS

85%

of CISOs admitted that they sacrificed security to quickly enable remote work.

79%

of CIOs are concerned that users might not follow security guidelines while working from home.

54%

of CISOs lack the visibility needed to ensure proper data protection.

CHAPTER 2

Shift in Cyber Security Concerns

To understand how organizations' security priorities were changed by the pandemic, we provided a predefined list of threats and asked respondents to choose the top three data security threats before their organizations went remote and after.

WHICH THREATS REMAIN CRITICAL?

Employee mistakes, including accidental improper sharing of data by employees and errors by admins, remain key concerns, holding nearly steady at over 60% of respondents. Both ransomware and phishing dropped slightly in the threat ranking but remain firmly on organizations' radar, with over 60% still naming them. That's wise, given how actively hackers have been employing these techniques to exploit people's fear and confusion, such as by distributing malicious emails that mention COVID-19.

WHAT HAS CHANGED IN THE THREAT LANDSCAPE?

Unsurprisingly, the percentage of respondents concerned about VPN exploitation has tripled, from 26% pre-pandemic to 85% now. The next biggest jump was misconfiguration of cloud services, which increased from 48% to 66%. Obviously, both findings are due to the fact that organizations now have to support remote employees.

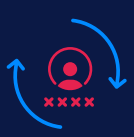
More organizations are also worried about deliberate employee misbehavior; data theft was mentioned by 66% of respondents, up from 54% pre-pandemic. This increase might be due to the massive staff reductions in the wake of the economic downturn and concern about departing employees taking corporate data.

Additionally, the recent large-scale phishing campaigns and data breaches enriched hackers' databases with more logon credentials. Since so many people re-use their passwords across sites, the problem of credential stuffing is becoming more acute; this is reflected by an increase of 11 percentage points in the survey results, from 55% to 66%.

ADDITIONAL HIGHLIGHTS

Among midsized organizations (100–1,000 employees), concern about credential stuffing grew from 53% to 80%.

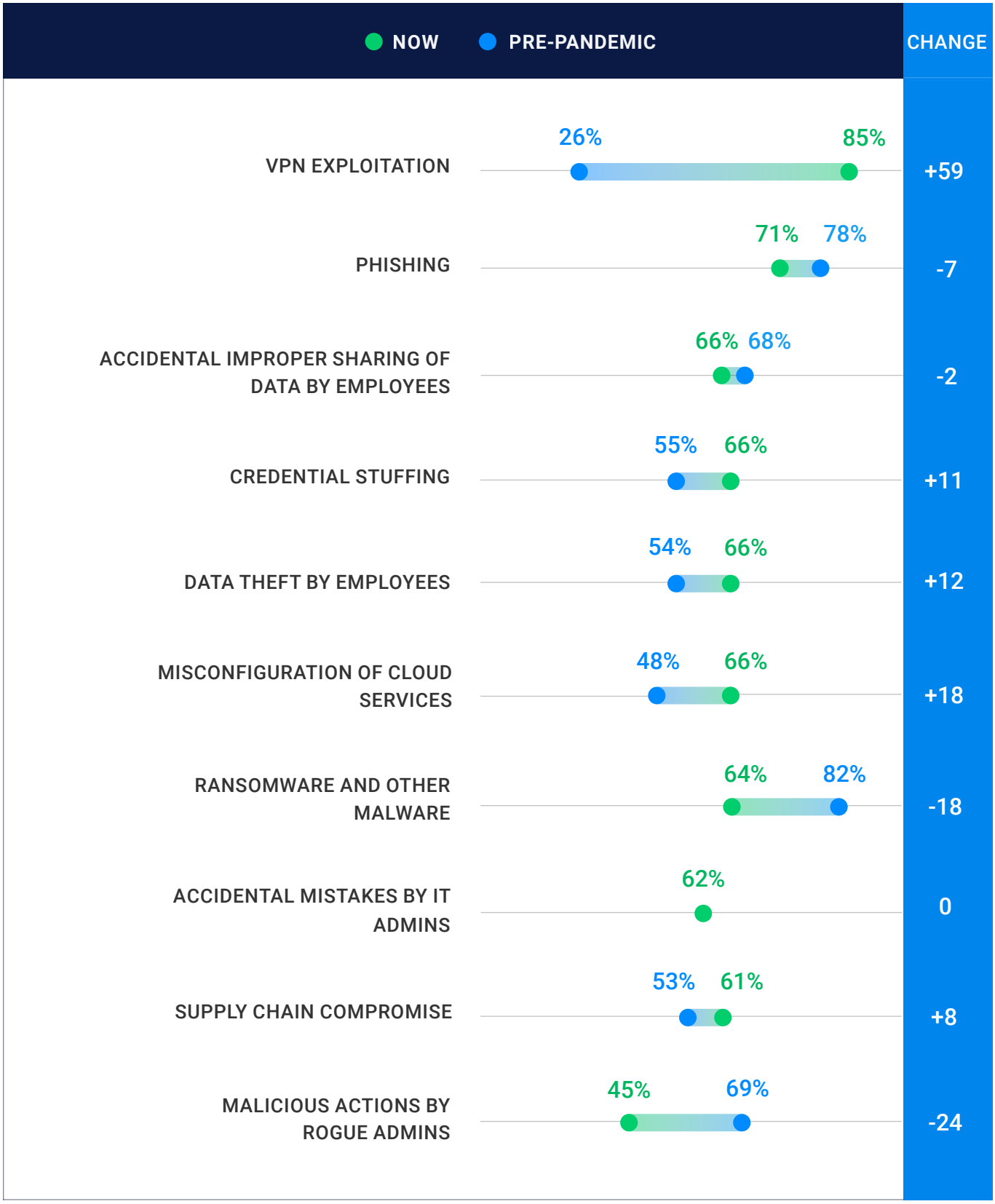
More enterprises (1,001+ employees) are now focused on the threat of data theft by employees; that result has increased from 44% pre-pandemic to 66% now.



The number of CISOs worried about credential stuffing has doubled, from 33% to 67%.

Concern about the threat that misconfiguration of cloud services poses to data security has nearly doubled among system administrators, from 34% to 66%.

Threats considered critical pre-pandemic and now



CHAPTER 3

Security Incidents Since WFH Began

TOP THREATS

For the survey, we listed a number of types of security incidents and asked respondents whether they had experienced any of them since their organizations went remote. The most common type of attack by far was phishing; nearly half of all organizations had dealt with phishing attacks. This is not a surprise, since authorities like the FBI have been reporting a huge number of COVID-related scams targeting remote employees. 86% of organizations were able to detect such attacks in minutes or hours, increasing their chances of minimizing the damage.

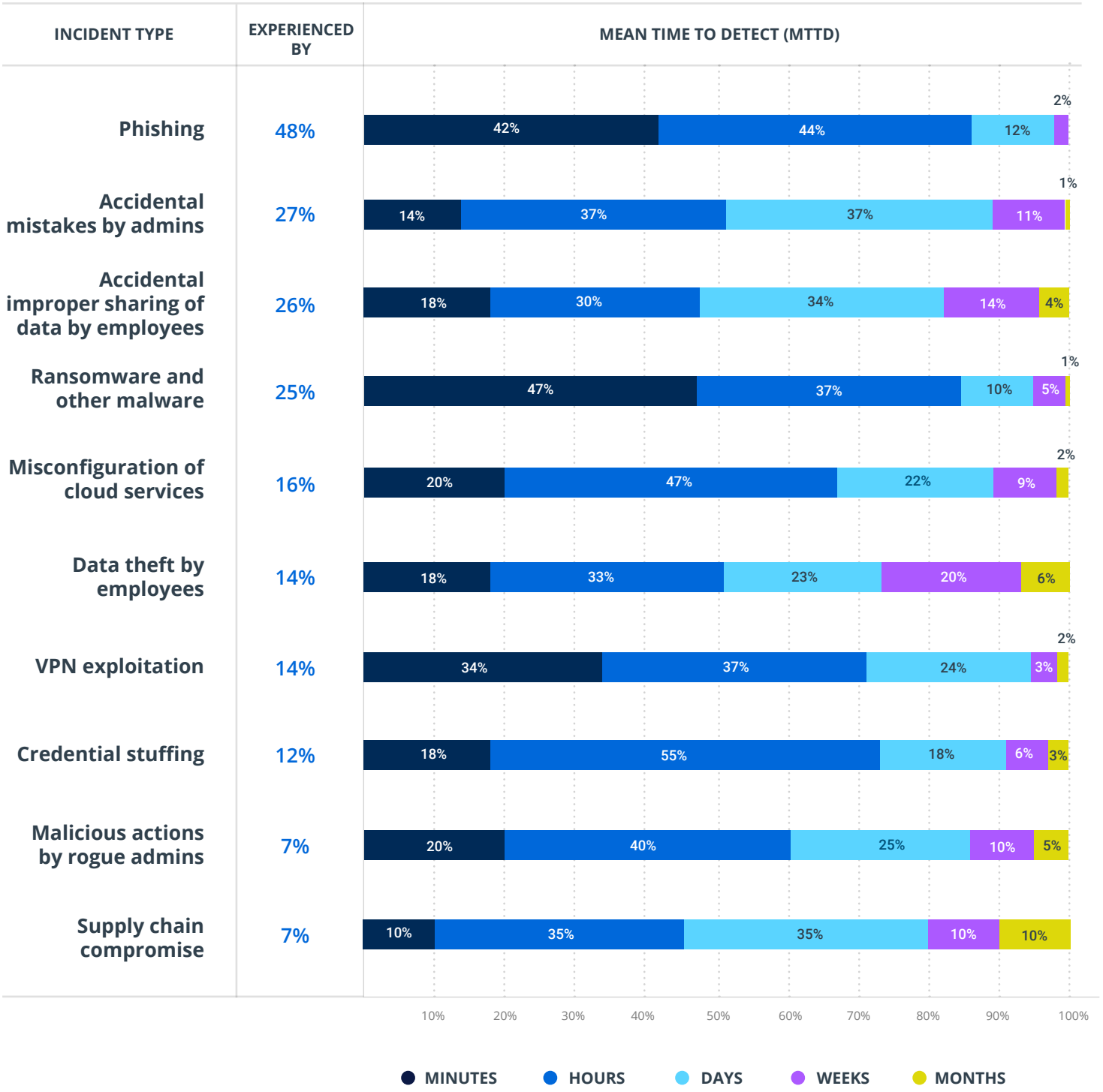
SLOWEST DETECTION TIMES

Every fourth organization suffered from mistakes by administrators, accidental data sharing by employees and ransomware. While most organizations were able to detect ransomware within minutes or hours, human errors were far more difficult to spot. In half of the cases, it took organizations days, weeks or months to detect those incidents, which obviously increases the associated risks.

Other incidents that organizations were slow to detect include data theft by employees and supply chain compromise. Although the latter was experienced by relatively few organizations, more than half of them failed to identify and mitigate the incident quickly. Cases in which a company fails to update its partners about a data breach are not that rare, so early detection of supply chain compromises is critical.

We highly advise all organizations to pay special attention to the detection of the following incidents: supply chain compromise, accidental improper data sharing by employees, data theft by employees, and accidental misconfigurations and other mistakes by administrators. Organizations should ensure their MTTD for these incidents is measured in minutes or hours, not days or weeks.

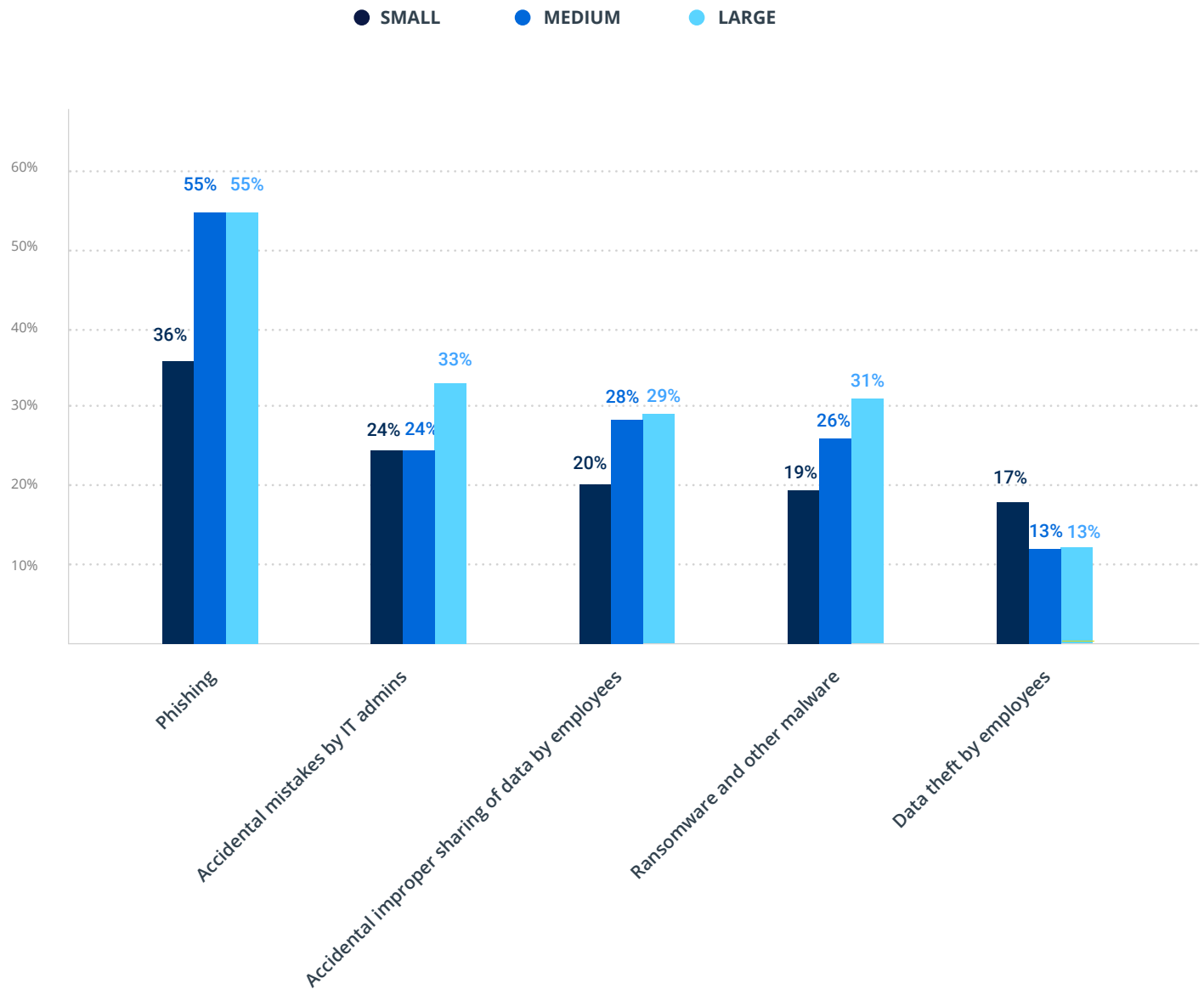
Most common cybersecurity incidents since organizations went remote



SECURITY INCIDENTS BY ORG SIZE

- 55% of mid-sized and large enterprises experienced phishing attacks since they moved their workforce remote, as compared to 36% of small organizations.
- The risk of being targeted by ransomware is also greater for medium and large businesses than for small companies. 31% of large enterprises reported suffering a ransomware attack.

Top 5 most common incidents by organization size



CHAPTER 4

Reporting on the State of Security

TOP METRICS USED

The majority (66%) of IT professionals regularly report on the state of cybersecurity to their leadership. Mainly these reports include:

- Incident statistics, such as number of incidents detected, number responded to, and mean time to resolve
- Vulnerability statistics, such as the number of vulnerabilities identified or patched, and the average time to patch
- General "state of cybersecurity" score, an average figure that sums up several cybersecurity metrics to track overall success

Incident and vulnerability statistics are raw numbers that often present limited value for decision-making. Therefore, many IT leaders are trying to create their own "state of cybersecurity score" to report on the success or failure of their implemented security measures. However, there are no standards, so each IT leader is left to their own devices. The survey shows that 56% of security professionals are trying to calculate some sort of average score. We expect that such high demand for an integral metric of cybersecurity will be addressed by the professional community and experts in the near future. 48% of respondents report the results of employee training, a major metric for tracking cybersecurity.

As the economic downturn unfolds, we expect more CFOs to be asking IT leaders to justify proposed expenses via a ROI analysis before approving the budget. 37% of organizations already try to calculate the total amount their organizations spend on cybersecurity. However, only about a quarter of respondents report detailed financial metrics like return on investment (ROI) and total cost of ownership (TCO).

TIME SPENT ON REPORTING

More broadly, 41% of respondents think that they spend too much time and effort on reporting than they should. This result clearly indicates the need for monitoring and reporting solutions that reduce manual work and provide IT professionals with straightforward summaries about the state of their cybersecurity. This should include dashboard and reports that can be easily shared with — and understood by — non-technical executives and the Board.

66% of respondents regularly report on the state of cybersecurity to their organization's executive leadership or board of directors.

Most common metrics to report on the state of cybersecurity

Incident statistics	61%
Vulnerability statistics	57%
State of cybersecurity score	56%
Employee training results	48%
Total amount spent	37%
Total cost of ownership	26%
Return on investment	22%

41% of respondents feel that IT teams spend more time and effort on reporting than they should.

RECOMMENDATIONS

Be ready to thwart phishing and ransomware attacks.

Since the pandemic began, more than half of organizations have experienced at least one phishing attack. One quarter report a ransomware attack; however, organizations may not know that employees' devices are compromised until they return to the office, so we might see the number of reported ransomware attacks to increase as organizations bring staff back on site.

The core best practices for mitigating these security risks include the following:

- Provide regular user training on how to identify suspicious links and attachments and how to report them.
- Enable continuous IT auditing with alerts on signs of ransomware in progress, such as unusual spikes of activity across file repositories.
- Harden data access governance by revoking excessive access rights.

Pivot to closing security gaps caused by the rapid switch to remote work.

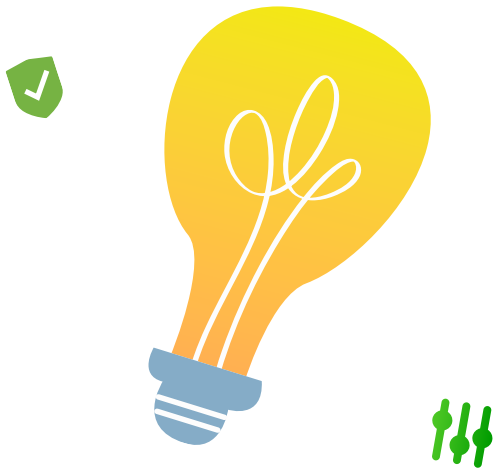
The swift transition to WFH forced many organizations to prioritize service availability over everything else. Now, IT leaders should revisit their previous decisions to see whether the tradeoffs they had to make might have created security gaps for hackers to exploit. They should start by documenting what access to which systems has changed since mid-March and what types of data those systems contain. Armed with this information, they can identify the risks to critical or regulated data, work with executive management to determine acceptable risk levels, and craft risk mitigation strategies.

Implement controls to minimize damage from admin mistakes.

Mistakes by admins, such as improper configurations and unwanted changes, are a leading cause of security incidents and business disruptions. One key reason is that organizations are slow to detect them — over 50% needed days, weeks or months to flag these incidents.

To mitigate the risk of breaches and downtime, organizations need to:

- Establish and rigorously enforce a least-privilege model.
- Utilize privileged access management (PAM) solutions to restrict admin activity.
- Automate change auditing across key IT systems to detect issues as they emerge.
- Conduct periodic reviews to spot any deviations in system configuration from a healthy baseline.



APPENDIX 1:

RESULTS BY VERTICAL

Below are the key findings in each of the verticals studied:

- Government
- Finance
- Healthcare
- Education

GOVERNMENT

NEARLY ONE IN THREE GOVERNMENT ORGANIZATIONS FEELS MORE VULNERABLE THAN BEFORE.

Among government agencies that feel that they are at greater risk, 86% are worried about more severe cyberattacks, which is the highest percentage among all the verticals in the survey. The next most frequently cited concern is employees ignoring security policies, which is a problem in every industry studied.

29% of agencies think they are at greater cybersecurity risk than before.

Security concerns of those who think they are at greater risk

Stronger or more frequent cyber attacks	86%
Users may ignore security guidelines	57%
Unexpected security gaps caused by WFH	43%
Sacrificed security in favor of availability	43%
Lack of visibility	14%

THE INSIDER THREAT IS SEEN AS POSING LESS RISK THAN EXTERNAL ATTACKS.

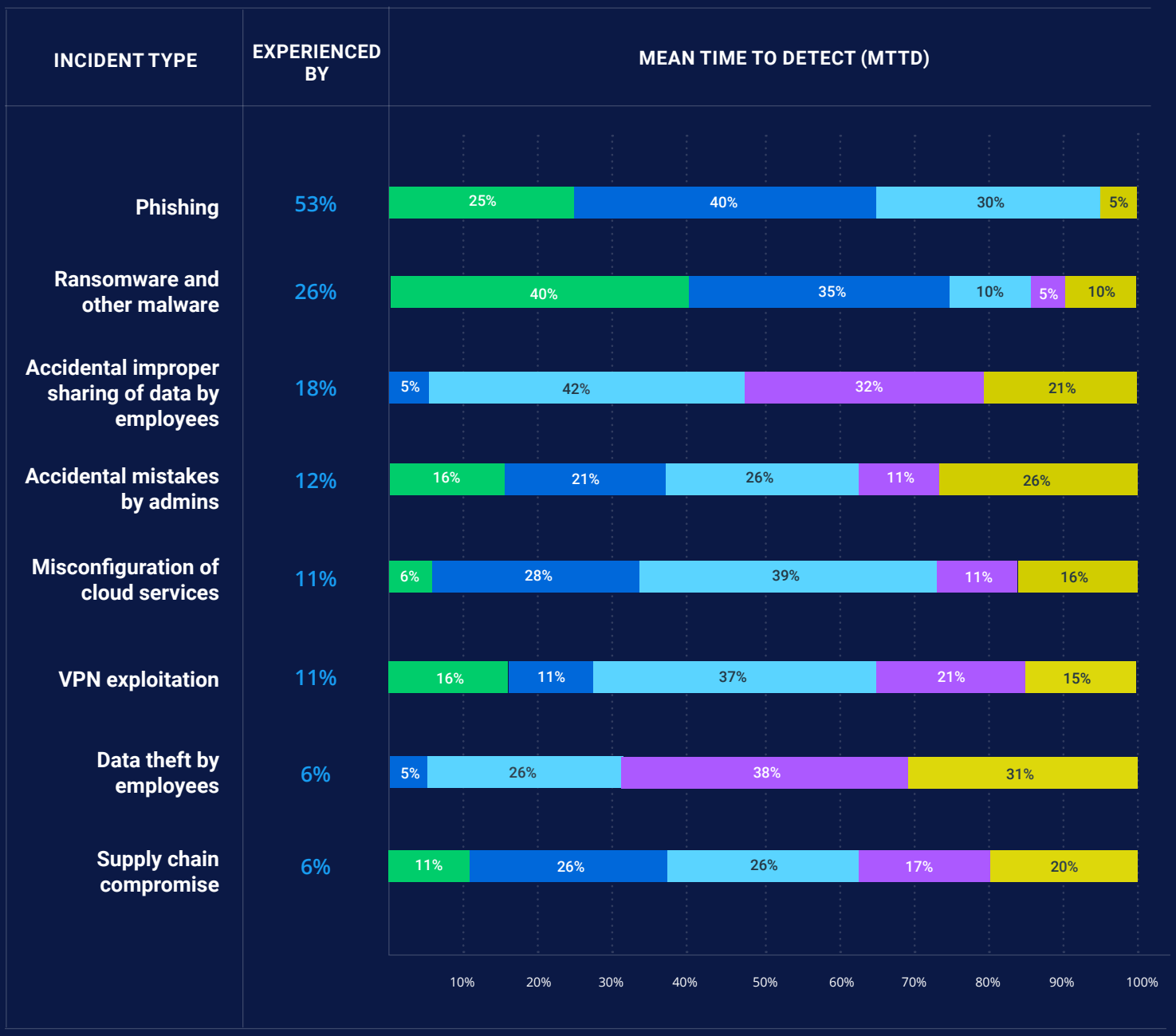
Today, public sector organizations are mostly concerned about external threats, such as VPN exploitation, supply chain compromise and credential stuffing. The insider threat is seen as much less pressing, except for cloud misconfigurations: The number of government organizations that say it is a top threat soared by 63 percentage points since the pandemic began.

Threats considered critical pre-pandemic and now

PHISHING AND RANSOMWARE WERE THE MOST COMMON INCIDENTS.

Organizations were less concerned about phishing and malware than before, which is surprising since these threats keep dominating the headlines. Fortunately, they have quite short MTTDs for these attacks. Improper data sharing is a top concern for every fifth organization; that number should probably be higher, since 53% required weeks or months to detect it.

Most common cybersecurity incidents since organizations went remote



EMPLOYEE TRAINING RESULTS ARE REPORTED BY HALF OF GOVERNMENT AGENCIES.

6 out of 10 IT teams in the public sector report on the state of cybersecurity to the upper management. As in the education vertical, none of the respondents estimate the ROI for security products in use. The top metrics they do use include incident and vulnerability statistics and the results of employee training. Given that top three incidents that the industry faced in recent months are associated with the human factor, the latter metric is especially important.

61% **of IT professionals regularly report on the state of cybersecurity to their executive leadership or board of directors.**

Most common metrics used to report on the state of cybersecurity

Incident statistics	64%
Vulnerability statistics	55%
Results of employee training	55%
A general “state of security” score	45%
Total cost of ownership of security products	18%
Total amount spent on cybersecurity	9%

FINANCE

MORE ORGANIZATIONS IMPROVED THEIR SECURITY POSTURE THAN IN ANY OTHER VERTICAL.

Almost half of financial organizations improved their security posture in the wake of the massive move to remote work, which is much higher than in other verticals. However, 30% say they are at greater cybersecurity risk than before. About two thirds of them fear that the rapid transition to remote work resulted in security gaps, and a similar number say that they sacrificed security in favor of availability, or that they believe cyberattacks have become stronger or more frequent.

30% **of financial organizations feel they are at greater cybersecurity risk than before.**

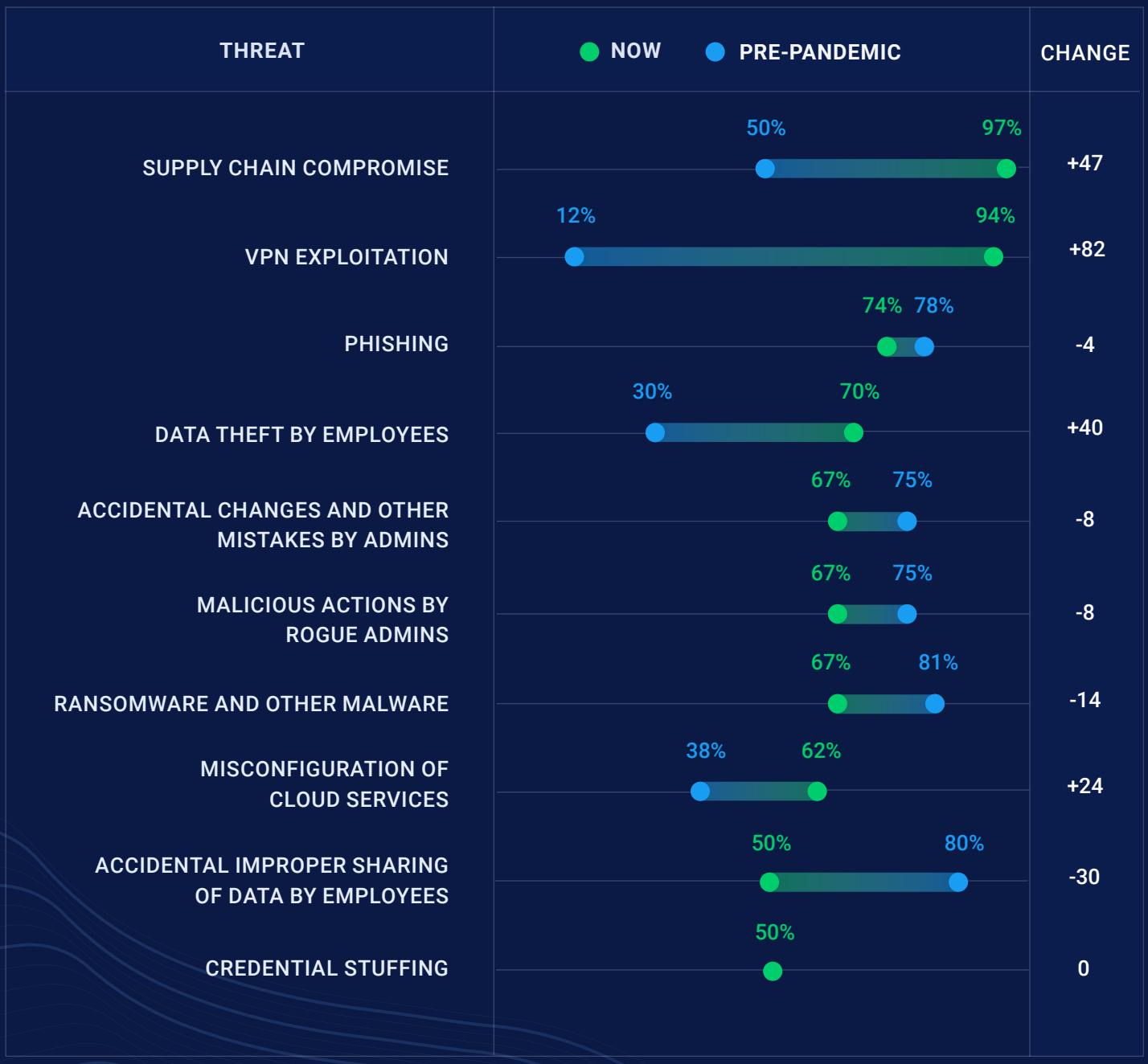
Security concerns of those who feel they are at greater risk

Stronger or more frequent cyber attacks	64%
Unexpected security gaps caused by WFH	64%
Sacrificed security in favor of availability	64%
Users may ignore security guidelines	55%
Lack of visibility	45%

CONCERN ABOUT DATA THEFT HAS DOUBLED.

Twice as many financial organizations are concerned about data theft by employees compared to pre-pandemic. Worry about misconfiguration of cloud services also increased significantly. But the biggest percentage point gains were associated with VPN exploitation, which skyrocketed from 12% to 94%, and supply chain compromise, which nearly doubled, from 50% to 97%.

Threats considered critical pre-pandemic and now



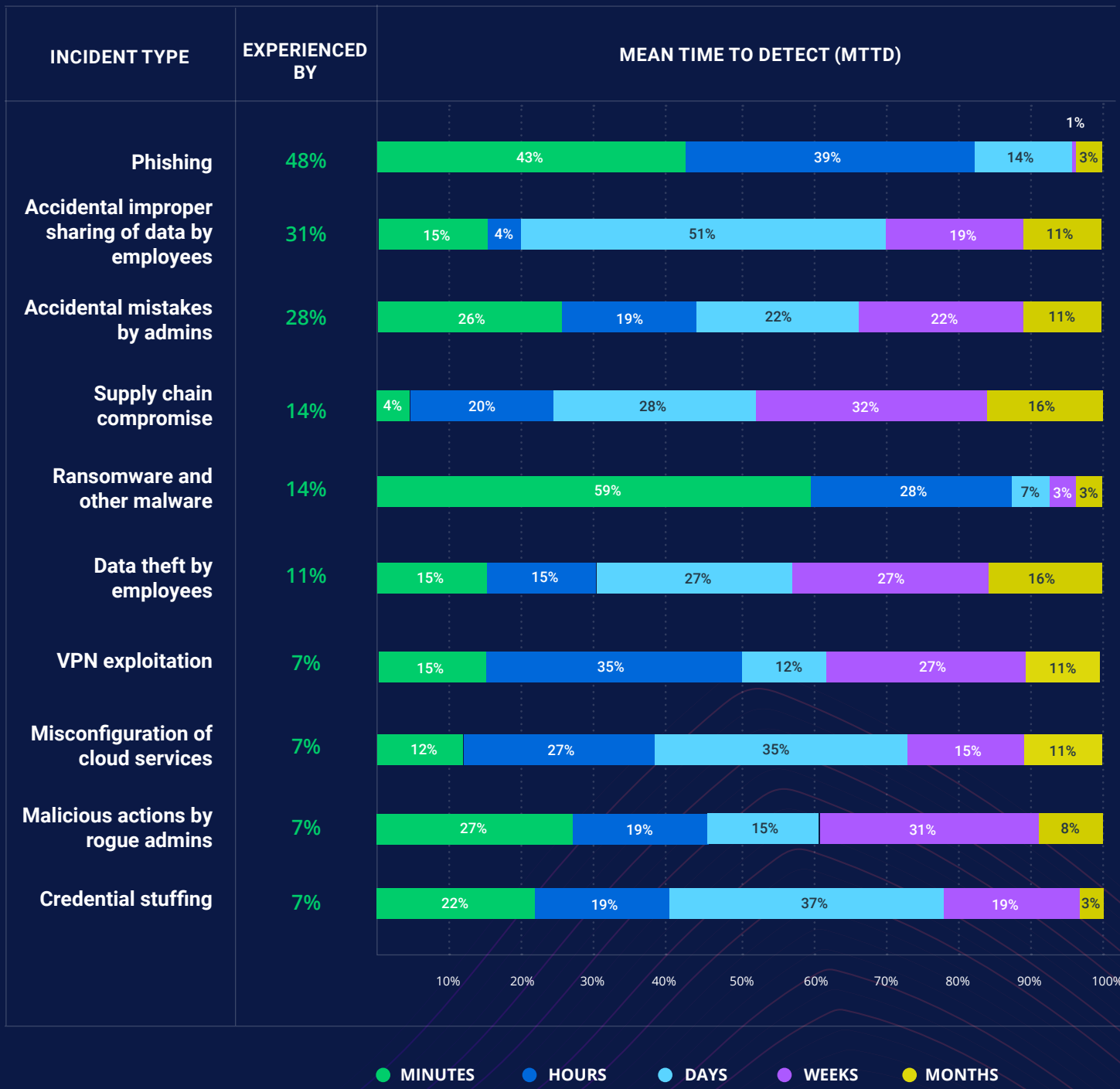
THE MOST COMMONLY REPORTED INCIDENTS INVOLVED HUMAN ERRORS.

Almost half of incidents in the financial sector were phishing attacks; 82% of them had a dwell time of minutes or hours.

The next two top incident types were human errors: improper data sharing and mistakes by IT staff. The absence of malicious intent does not mean an incident is harmless, so it is alarming how slow respondents were to detect them.

Also noteworthy is that the financial vertical experienced data theft by employees, VPN exploitation and supply chain compromise, yet half of respondents reported an MTTD of days, weeks and months for these types of incidents.

Most common cybersecurity incidents since organizations went remote



90% REGULARLY REPORT ON CYBERSECURITY.

Nine out of ten organizations in the financial sector regularly report on cybersecurity to senior management, which is the record among all industries analyzed. When it comes to security reporting, financial organizations rely less on dollar estimates and more on incident and vulnerability statistics, a general “state of security” score, and the results of employee training. The latter is particularly relevant, given the increase in phishing and incidents caused by user mistakes. However, 31% of respondents feel that reporting takes more time and effort than it should.

90% **of IT professionals regularly report on the state of cybersecurity to their executive leadership or board of directors.**

Most common metrics used to report on the state of cybersecurity

Incident statistics	81%
Vulnerability statistics	73%
Results of employee training	46%
A general “state of security” score	46%
Total amount spent on cybersecurity	38%
Return on investment for security products	31%
Total cost of ownership of security products	23%

HEALTHCARE

RELATIVELY FEW HEALTHCARE ORGANIZATIONS SAY THEY ARE AT GREATER RISK NOW.

Healthcare organizations are split almost evenly among those who improved their cybersecurity (39%) and those who say that the threat landscape hasn't really changed for them since the pandemic (43%). Only 18% say they are at greater cybersecurity risk, which is the lowest number of all industries analyzed in this report. The majority of healthcare organizations are concerned about stronger or more frequent cyberattacks and users trying to circumvent security policies.

18% of healthcare organizations feel they are at greater cybersecurity risk than before.

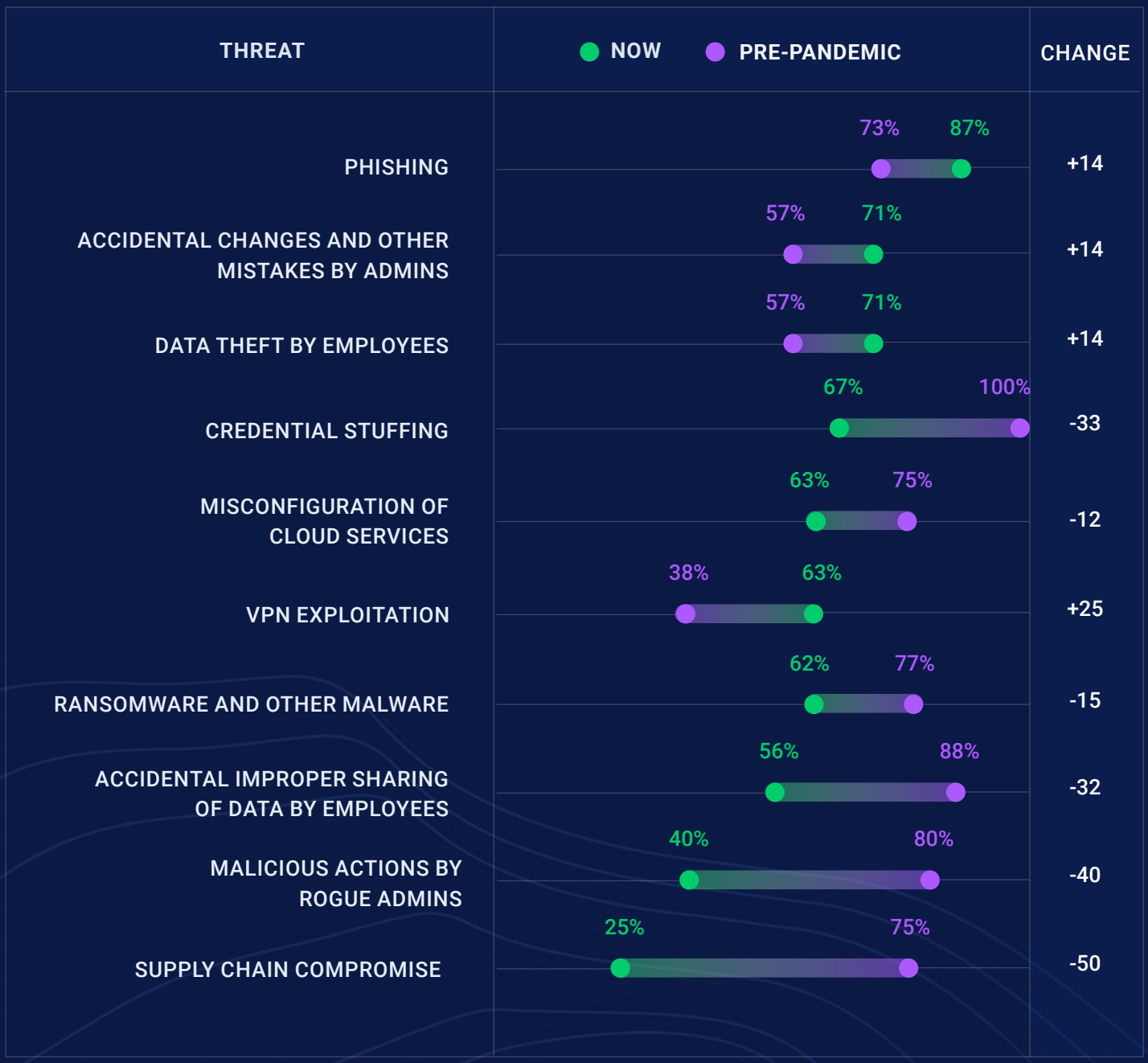
Security concerns of those who feel they are at greater risk

Stronger or more frequent cyber attacks	60%
Users may ignore security guidelines	60%
Unexpected security gaps caused by WFH	40%
Sacrificed security in favor of availability	20%

PHISHING, ADMIN MISTAKES AND DATA THEFT HAVE BECOME THE TOP CONCERNS.

Healthcare organizations were more worried about phishing attacks than other industries. Interestingly, before the pandemic, they were primarily concerned about employees accidently sharing sensitive data and admins going rogue; today, they are worried about the polar opposites: data theft by employees and admins making mistakes. Also of interest is the fact that healthcare has fewer organizations concerned about the threat of VPN exploitation than any other industry covered in this report.

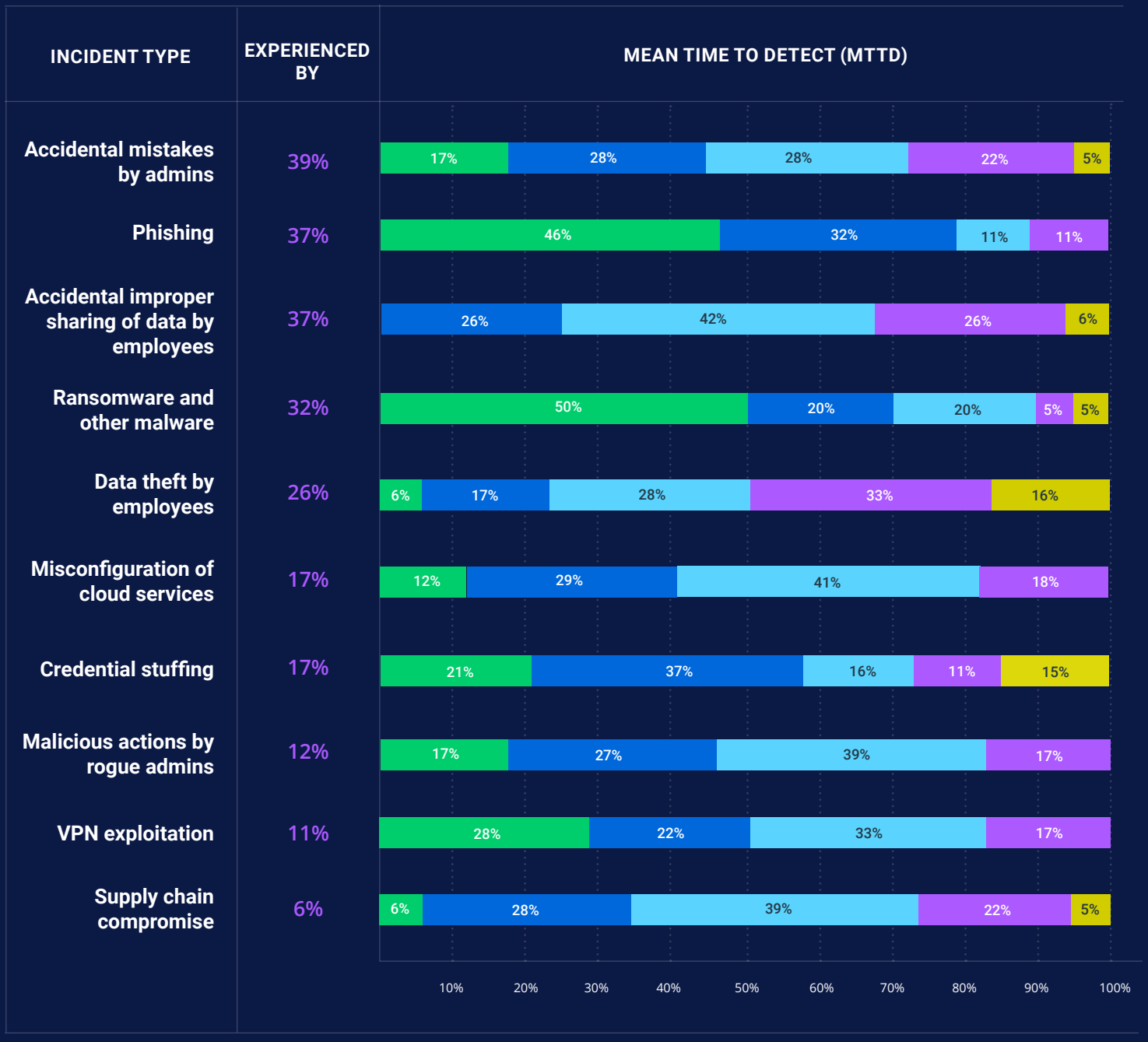
Threats considered critical pre-pandemic and now



IMPROPER DATA SHARING IS SEEN AS MORE CRITICAL THAN EXPECTED.

Every third healthcare organization surveyed experienced a ransomware attack, which is the highest result among all the verticals. 70% of them were able to detect it in minutes or hours. Among the top incidents suffered by healthcare organizations were data theft by employees and admin mistakes — the exact threats they are most concerned about. Unfortunately, they were way too slow in detecting data theft; it took weeks or months for half of them. Also, they should not continue to underestimate the threat of improper data sharing: It was the other incident type in the top three, yet no respondent detected it in minutes and only a quarter spotted it within hours.

Most common cybersecurity incidents since organizations went remote



8 OUT OF 10 HEALTHCARE ORGANIZATIONS REPORT ON CYBERSECURITY.

The vast majority of healthcare IT pros report on the state of cybersecurity to their executive leadership or board, and 47% of them are convinced that it takes more time than it should. The key metrics they present are vulnerability statistics, a "state of security" score and the total amount spent on cybersecurity. Results of employee training are reported by only 27%, which is the lowest number of all the verticals.

79% **of IT professionals regularly report on the state of cybersecurity to their executive leadership or board of directors.**

Most common metrics used to report on the state of cybersecurity

Vulnerability statistics	60%
Total amount spent on cybersecurity	47%
A general "state of security" score	47%
Total cost of ownership of security products	40%
Incident statistics	40%
Results of employee training	27%
Return on investment for security products	13%

EDUCATION

AMONG ALL VERTICALS, EDUCATION TOPPED THE LIST IN FEELING AT GREATER RISK.

33% of educational organizations say they are more vulnerable to cyber threats than they were pre-pandemic, which is higher than any other vertical. 89% of them say they might have new security gaps caused by the rapid transition to remote work — again the highest finding among all industries analyzed. Moreover, 78% of educational institutions are concerned users may not follow security guidance when working from home.

33% of education organizations feel they are at greater cybersecurity risk than before.

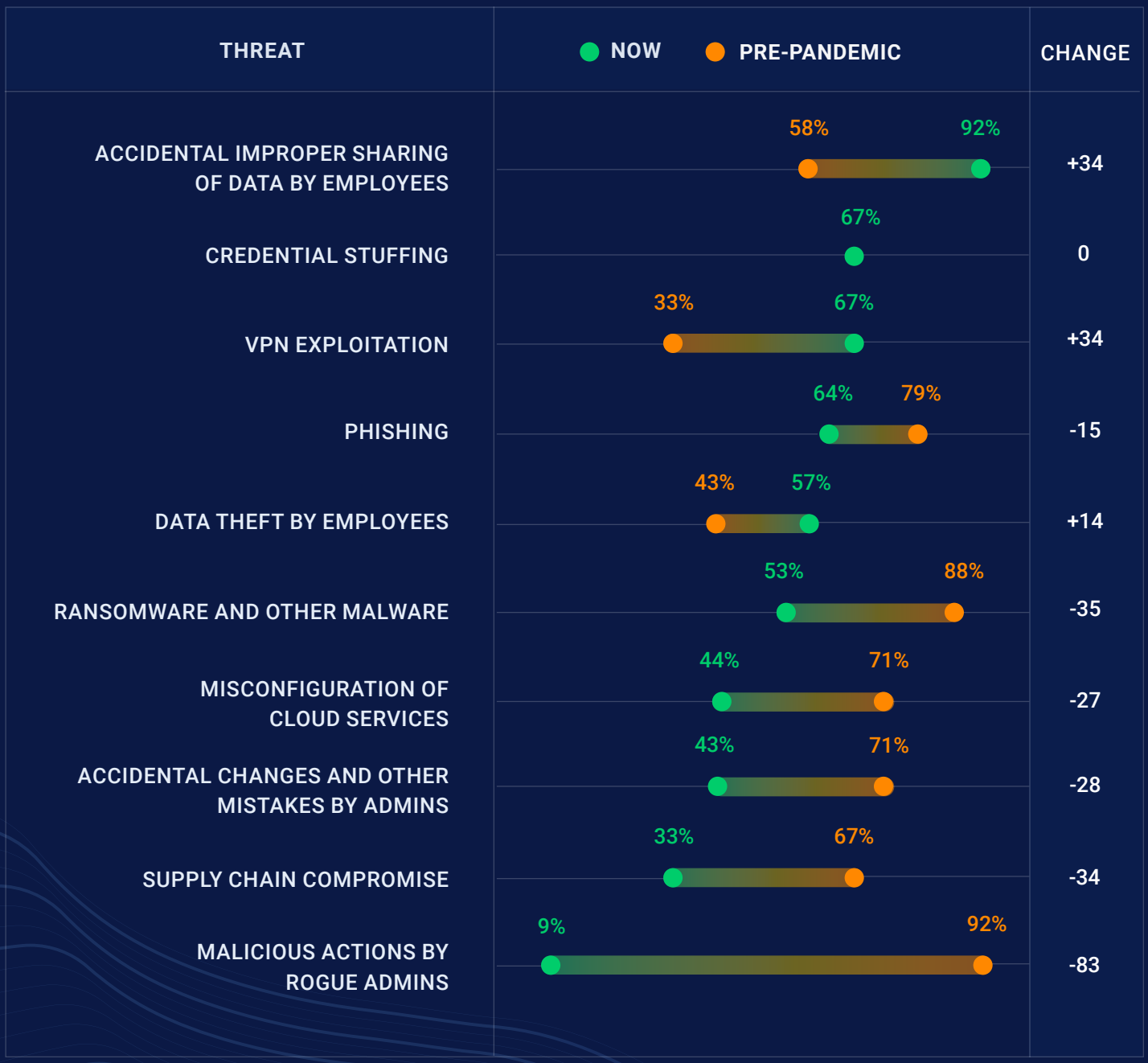
Security concerns of those who feel they are at greater risk

Unexpected security gaps caused by WFH	89%
Users may ignore security guidelines	78%
Stronger or more frequent cyber attacks	56%
Sacrificed security in favor of availability	33%
Lack of visibility	33%

REGULAR EMPLOYEES ARE NOW SEEN AS THE MAJOR SOURCE OF RISK.

Prior to the pandemic, educational organizations were mainly concerned about malicious actions by rogue admins, malware and phishing. Today, accidental data sharing, VPN exploitation and credential stuffing top the list.

Threats considered critical pre-pandemic and now

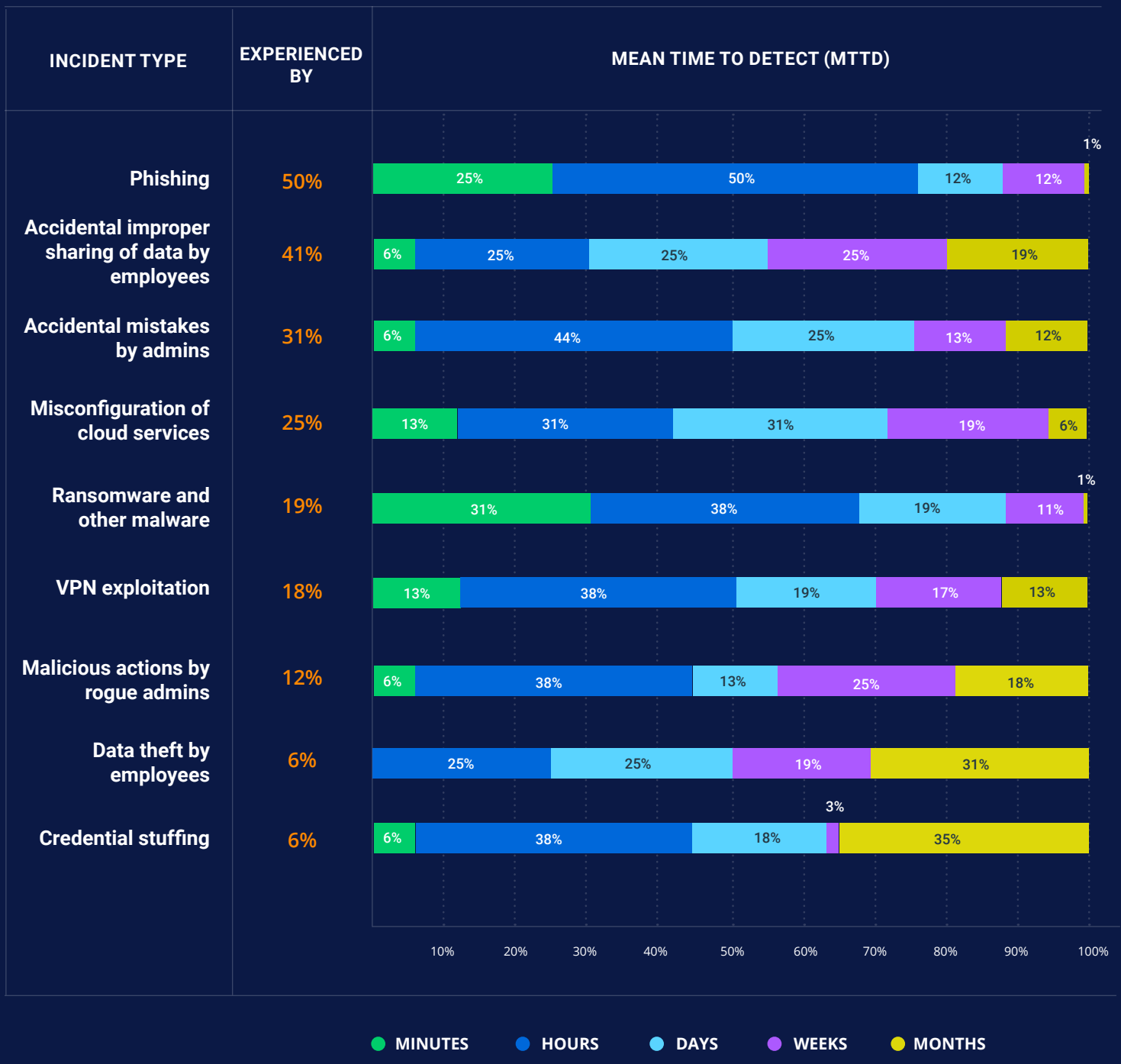


MALICIOUS ACTIVITY HAS THE LONGEST DWELL TIME.

In the first three months after the global transition to remote work, 50% of educational organizations experienced phishing attacks. 75% of respondents were able to detect them in minutes or hours.

Next most common were incidents related to employee negligence, such as accidental data sharing and mistakes by IT personnel. These internal threats had longer MTTD, which might explain why they moved up in the threat ranking. Though malicious activity was not that common, it is worrisome that detection of data theft and rogue admin activity took weeks or months in most cases.

Most common cybersecurity incidents since organizations went remote



MORE EDUCATIONAL INSTITUTIONS RELY ON THE TOTAL AMOUNT OF SECURITY EXPENSES THAN IN OTHER SECTORS.

Less than half of educational organizations report on cybersecurity to executive leadership. Among those that do, 45% provide information on the amount of money spent on cybersecurity, which is a higher percentage than in other industries. At the same time, none of the respondents said they estimate the ROI for security solutions.

44% of IT professionals regularly report on the state of cybersecurity to their executive leadership or board of directors.

Most common metrics used to report on the state of cybersecurity

Total amount spent on cybersecurity	45%
Results of employee training	43%
Incident statistics	43%
A general “state of security” score	29%
Total cost of ownership of security products	14%
Vulnerability statistics	14%
Return on investment for security products	0%

APPENDIX 2:

RESULTS BY GEOGRAPHICAL REGION

Below are the key results for each geographic region:

- North America
- Europe, Middle East and Africa (EMEA)
- Asia-Pacific (APAC)

NORTH AMERICA

24% OF ORGANIZATIONS FEEL THEY ARE EXPOSED TO GREATER SECURITY RISKS THAN THEY WERE PRE-PANDEMIC.

Every fourth organization in North America feels that they are exposed to more risks than before the pandemic. Of them, 77% are concerned about more severe cyberattacks and 64% are worried about new security gaps caused by the rapid shift to remote work and users ignoring security guidelines.

As for cyber threats, North American organizations express more concern about VPN exploitation (up from 26% pre-pandemic to 84% now) and cloud misconfiguration (up from 49% to 66%).

However, the most common incidents these organizations experienced in the first three months were phishing attacks (51%) and IT admin mistakes (24%).

Phishing attacks were generally detected in minutes or hours; IT staff mistakes were harder to spot — over 40% needed days, weeks or months to detect them.

69% of respondents in North America report on the state of cybersecurity to the board, and 36% of them are convinced reporting takes more time and effort than it should. Vulnerability and incident statistics are the most common security metrics, followed by a general cybersecurity score.

77% **are concerned about stronger or more frequent cyberattacks.**

64% **admit that the rapid transition to WHF might have caused security gaps.**

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

50% OF EMEA ORGANIZATIONS EXPERIENCED A PHISHING ATTACK, AND 30% HAD INCIDENTS CAUSED BY ADMINS' MISTAKES.

Nearly a third of EMEA organizations (28%) feel they're at greater cyber risk now than pre-pandemic. This is the highest number of all regions analyzed. 61% of them believe that they might have security gaps caused by the rapid transition to remote work. The top 3 cybersecurity concerns named by EMEA respondents were VPN exploitation (88%), phishing (82%) and improper data sharing by employees (77%). Interestingly, VPN exploitation soared from just 27% to the top of the list.

In the first three months of the pandemic, 50% of EMEA organizations suffered a phishing attack; 30% had incidents caused by admins' mistakes; and 28% experienced insecure data sharing by employees. Mistakes by admins and data theft by employees were the hardest incidents to detect, with about two thirds of organizations spending days, weeks or months to flag them. Though only 18% of EMEA organizations experienced either data theft by employees or supply chain compromise, it is worrisome that 63% of respondents indicate they needed days, months or weeks to detect these incidents.

The majority (63%) of EMEA respondents regularly report on the state of cybersecurity. 69% report incident statistics, but only a few provide financial numbers such as return on investment (19%) and total cost of ownership (16%).

55% of EMEA organizations are worried that users may ignore security guidelines.

76% are concerned about the risk of data theft by employees. This number is up from 60% pre-pandemic.

ASIA-PACIFIC (APAC)

MORE THAN HALF OF INSECURE DATA SHARING INCIDENTS REMAINED UNDISCOVERED FOR DAYS, WEEKS OR MONTHS.

Only 17% of APAC organizations feel they are at greater risk now compared to pre-pandemic, which is the lowest number among other regions. 91% of them are concerned about possible security gaps caused by the rapid transition to remote work.

Three threats soared in the rankings since the COVID-19 outbreak: VPN exploitation (from 29% to 79%), misconfiguration of cloud services (from 32% to 73%), and credential stuffing (from 33% to 68%).

During the past three months, 37% of APAC organizations had unauthorized data sharing incidents. Sadly, 54% of them needed days, weeks or months to detect these incidents. 57% of the respondents required equally long to flag data theft by insiders and VPN exploitation; even though these incidents happened in just 20% of the surveyed organizations, such poor detection capability is worrying, since it gives attackers time to harvest vast amounts of sensitive data from the network.

69% of APAC organizations regularly report on cybersecurity to their executive leadership teams. However, the majority of them do not provide financial estimates regarding their cybersecurity efforts; they tend to use formal metrics like incident statistics. Only 12% calculate the return on investment for the tools and services they use.

41% of the APAC organizations suffered from ransomware in the past months.

64% indicate their approach to cybersecurity reporting is inefficient as they spend more time on reporting than they should.

APPENDIX 3:

RESULTS BY COUNTRY

Below are the key results for the following countries:

- United States
- United Kingdom
- France
- Germany

UNITED STATES

74% OF U.S. ORGANIZATIONS SAY THAT CYBERATTACKS HAVE BECOME STRONGER AND MORE FREQUENT.

It is encouraging that 43% of organizations in the U.S. managed to increase their security posture since the pandemic began. Those who say they are at greater risk than before are worried that cyberattacks have become stronger or more frequent.

22% of U.S. organizations feel they are at greater cybersecurity risk than before.

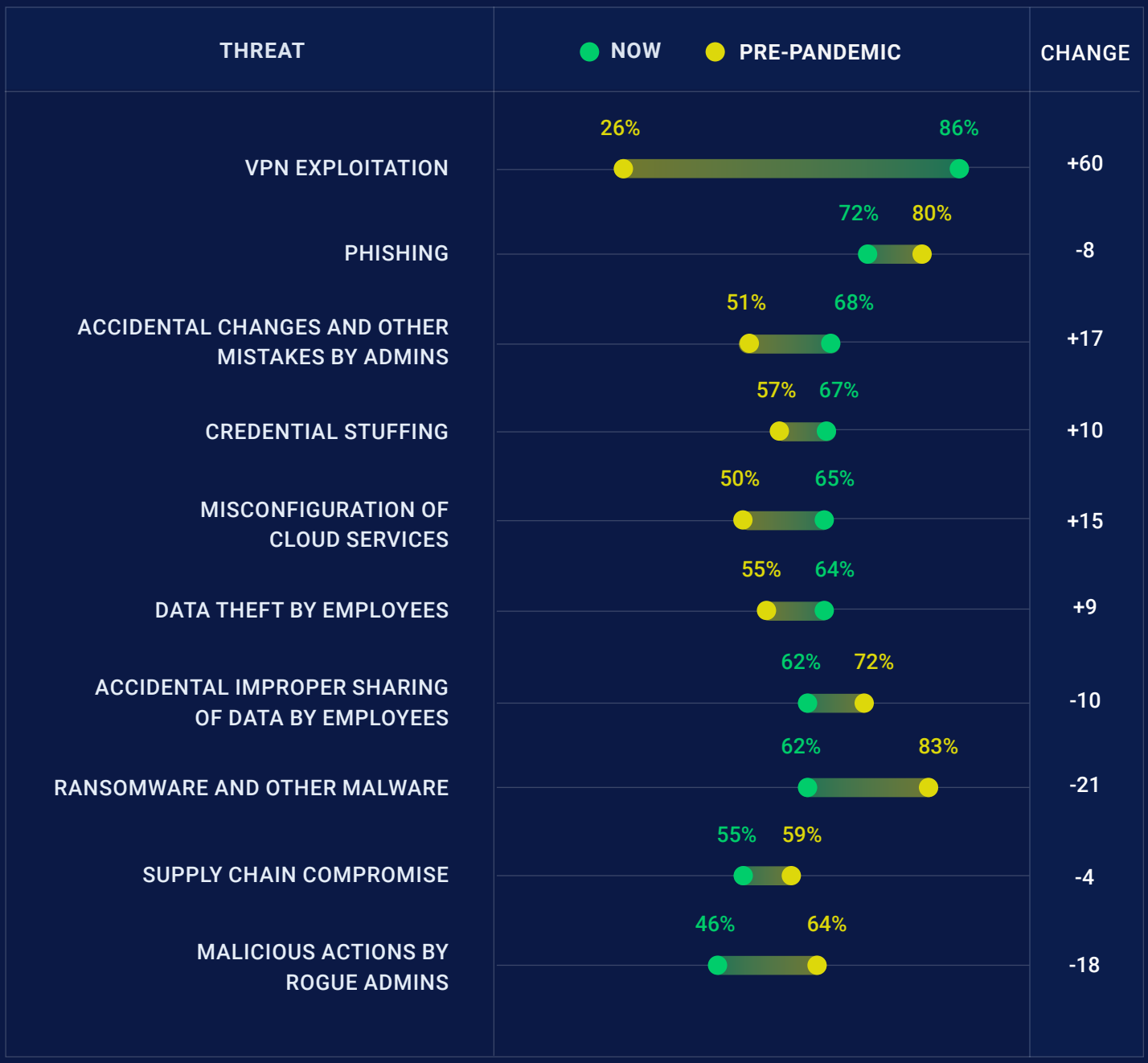
Security concerns of those who think they are at greater risk

Stronger or more frequent cyber attacks	74%
Unexpected security gaps caused by WFH	60%
Users may ignore security guidelines	63%
Sacrificed security in favor of availability	43%
Lack of visibility	34%

VPN EXPLOITATION AND PHISHING ARE THE TOP CONCERNS IN THE U.S.

Fear of malware, the top threat before the pandemic, has been replaced by concerns about VPN vulnerabilities, which skyrocketed 60 percentage points. A spike in concern about admin mistakes and cloud misconfigurations brought those threats up nearly level with phishing, which slipped a little and now stands at 72%.

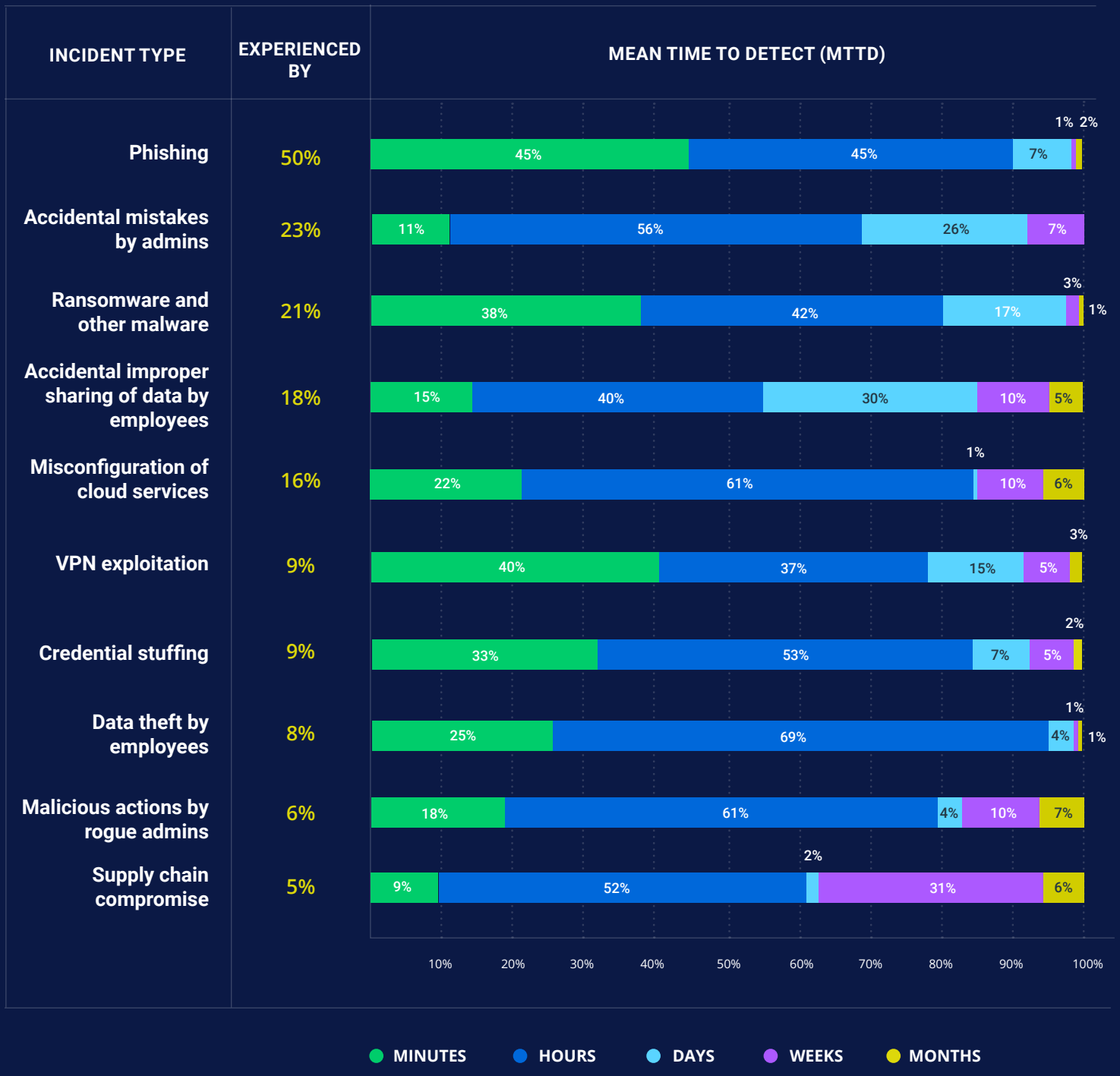
Threats considered critical pre-pandemic and now



UNAUTHORIZED DATA SHARING IS THE HARDEST THREAT TO DETECT.

The fears about phishing were justified, as half of organizations in the U.S. experienced at least one phishing attack in the first three months of the pandemic. They were mostly able to spot these attacks in minutes or hours. However, the reduced concern about malware was less apt; 21% of organizations were targeted with ransomware or other malware. Another common incident, accidental improper data sharing, was one of the slowest to be spotted — 40% needed days or weeks to detect it, and 5% required months.

Most common cybersecurity incidents since organizations went remote



7 OUT OF 10 ORGANIZATIONS IN THE U.S. REPORT ON CYBERSECURITY.

Most U.S. IT and security teams report on the state of cybersecurity to their management or the board. The key metrics they present include vulnerability and incident statistics, a general state of security score, and results of employee training. Financial metrics, such as ROI and TCO, are reported by less than a third of respondents.

69% of IT professionals in the U.S. regularly report on the state of cybersecurity to their executive leadership or board of directors.

Most common metrics used to report on the state of cybersecurity

Vulnerability statistics	59%
Incident statistics	54%
Results of employee training	53%
A general “state of security” score	53%
Total amount spent on cybersecurity	43%
Total cost of ownership of security products	30%
Return on investment for security products	23%

UNITED KINGDOM

HALF OF RESPONDENTS FEEL THEY ARE AT GREATER RISK DUE TO ESCALATING CYBER THREATS.

Among UK organizations, a similar share of respondents found themselves at greater risk (43%) as more secure (42%). 97% of those who feel they are at greater risk named escalating cyber attacks as their major concern.

43% of UK organizations are at greater cybersecurity risk than before.

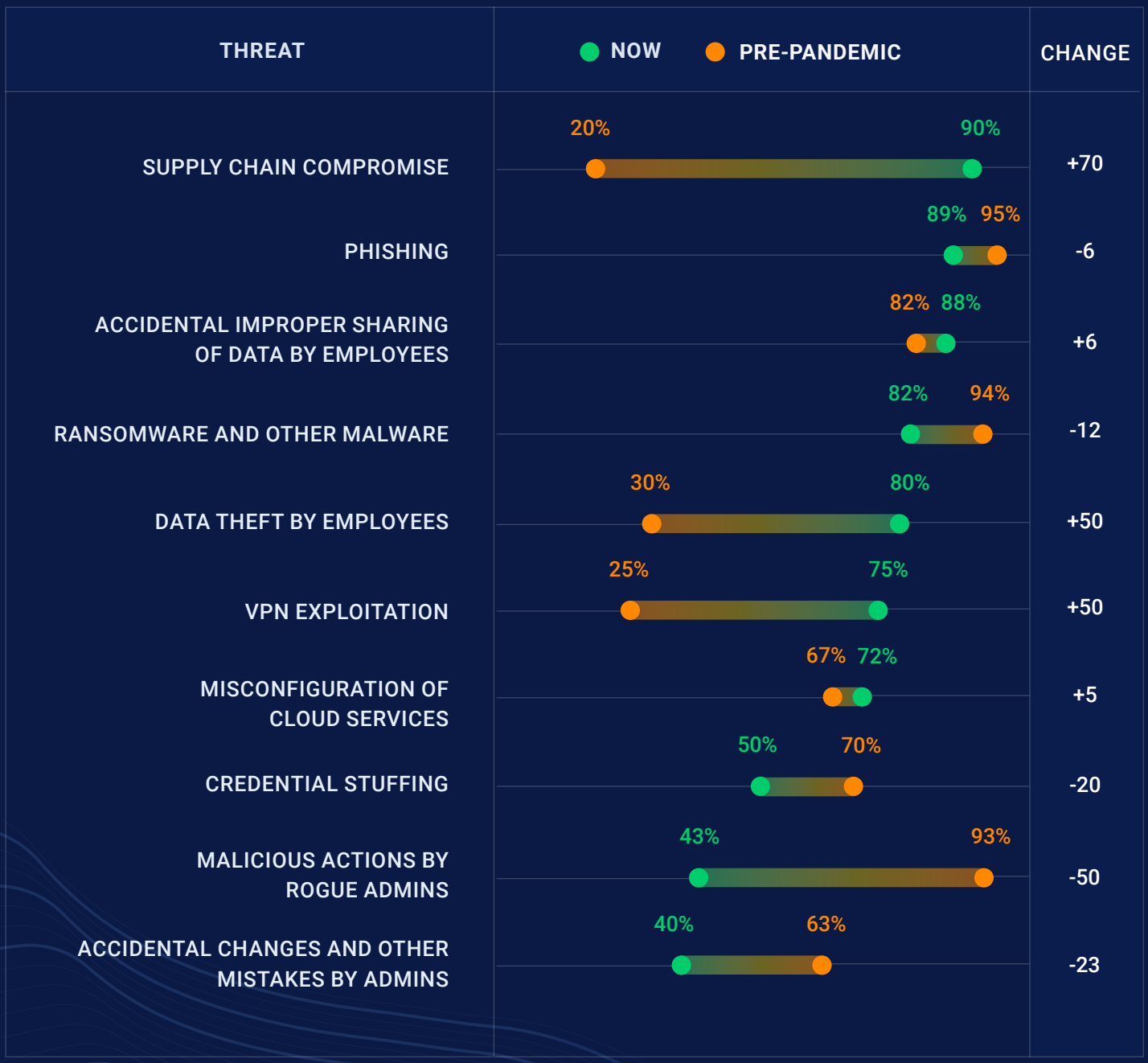
Security concerns of those who feel they are at greater risk

Stronger or more frequent cyber attacks	97%
Unexpected security gaps caused by WFH	82%
Users may ignore security guidelines	76%
Lack of visibility	40%
Sacrificed security in favor of availability	20%

CONCERN ABOUT SUPPLY CHAIN COMPROMISE SOARED AFTER THE PANDEMIC BEGAN.

UK respondents are mainly concerned about supply chain compromise (90%), phishing (89%) and accidental data sharing by employees (88%). Though the latter two threats were top concerns before pandemic, worry about supply chain compromise soared from just 20% pre-pandemic. Other types of threats that jumped tremendously in the ranking were data theft by employees and VPN exploitation.

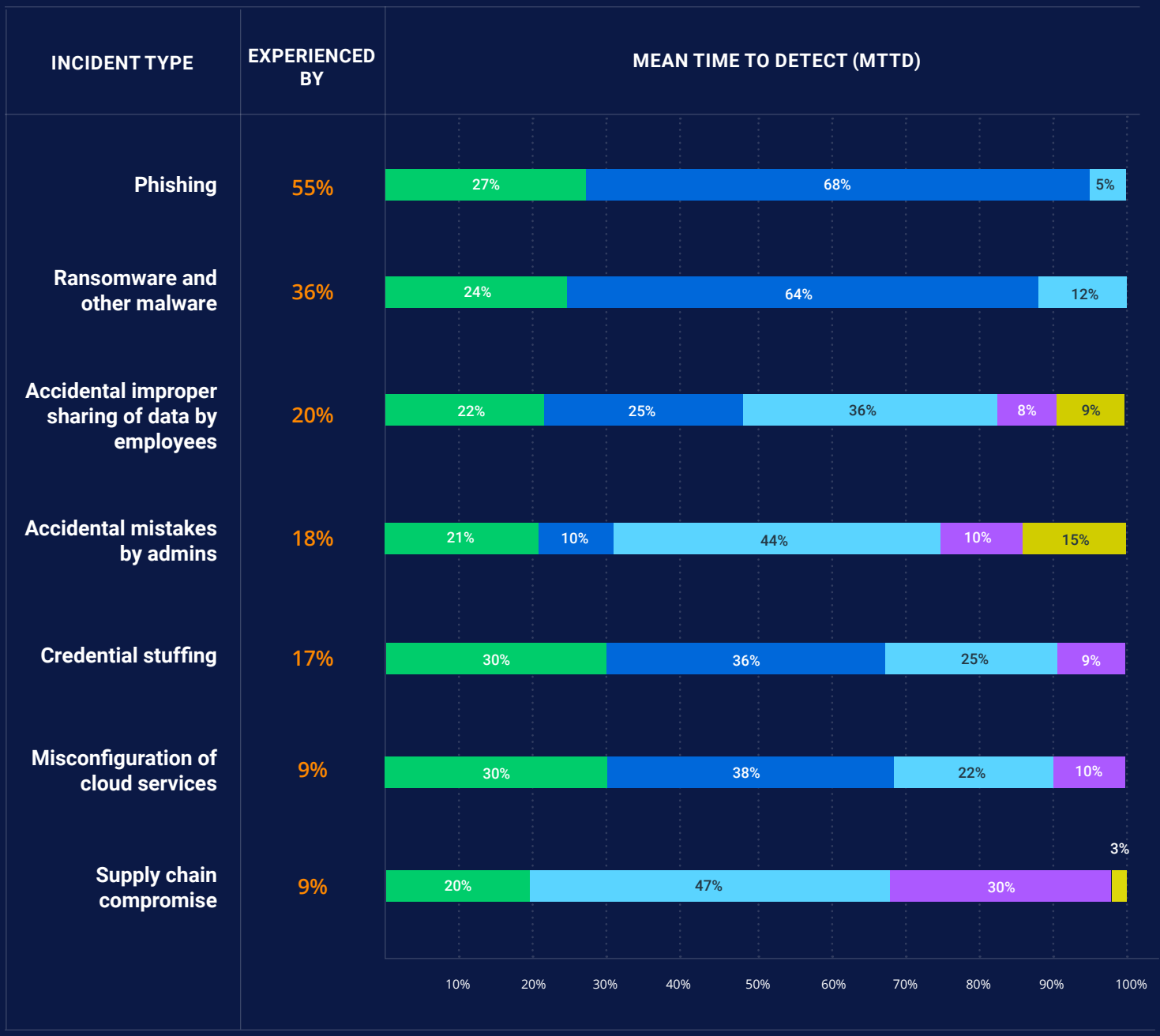
Threats considered critical pre-pandemic and now



MISTAKES BY ADMINS AND SUPPLY CHAIN COMPROMISES TOOK THE LONGEST TO DETECT.

In the first three months of the pandemic, more than half of UK organizations experienced phishing, and more than a third suffered a malware attack. Most of them needed hours to detect these incidents —long enough for attackers to steal or encrypt valuable data. More worrying, a quarter of incidents caused by admin mistakes and supply chain compromises remained undiscovered for weeks or even months.

Most common cybersecurity incidents since organizations went remote



THE MOST COMMON METRIC USED IN CYBERSECURITY REPORTING IS INCIDENT STATISTICS.

82% of the UK respondents regularly report on the state of cybersecurity to their executive leadership team, which is the highest of any country we analyzed in this report. The majority use incident statistics (95%) or a general "state of cybersecurity" score (75%). Although only one quarter calculate the impact of their cybersecurity efforts in financial terms like ROI, that's more than any other country analyzed in this report, which indicates that UK organizations are more inclined to analyze the financial impact of their security efforts.

82% **of IT professionals in the UK regularly report on the state of cybersecurity to their executive leadership or board of directors.**

Most common metrics used to report on the state of cybersecurity

Incident statistics	95%
A general "state of security" score	75%
Results of employee training	70%
Vulnerability statistics	50%
Total amount spent on cybersecurity	38%
Return on investment for security products	25%
TTotal cost of ownership of security products	13%

FRANCE

ORGANIZATIONS ARE CONCERNED ABOUT EMPLOYEE NEGLIGENCE.

One fourth of French organizations say they are at greater cybersecurity risk now than before the pandemic, while 53% didn't notice any change. 80% of those who feel at greater risk are worried that employees might not follow security guidelines.

26% of French organizations feel they are at greater cybersecurity risk than before.

Security concerns of those who feel they are at greater risk

Users may ignore security guidelines	80%
Unexpected security gaps caused by WFH	43%
Sacrificed security in favor of availability	40%
More vulnerable to cyber threats than before	36%
Stronger or more frequent cyber attacks	21%
Lack of visibility	20%

CONCERN ABOUT VPN EXPLOITATION SOARED AFTER THE PANDEMIC BEGAN.

In France, just like in the rest of the world, the transition to remote work has led to a tremendous increase in concern about VPN exploitation. Worry about misconfiguration of cloud services has also soared. The third most cited cybersecurity threat is the risk of admins' mistakes; however, this was already a top concern before the pandemic.

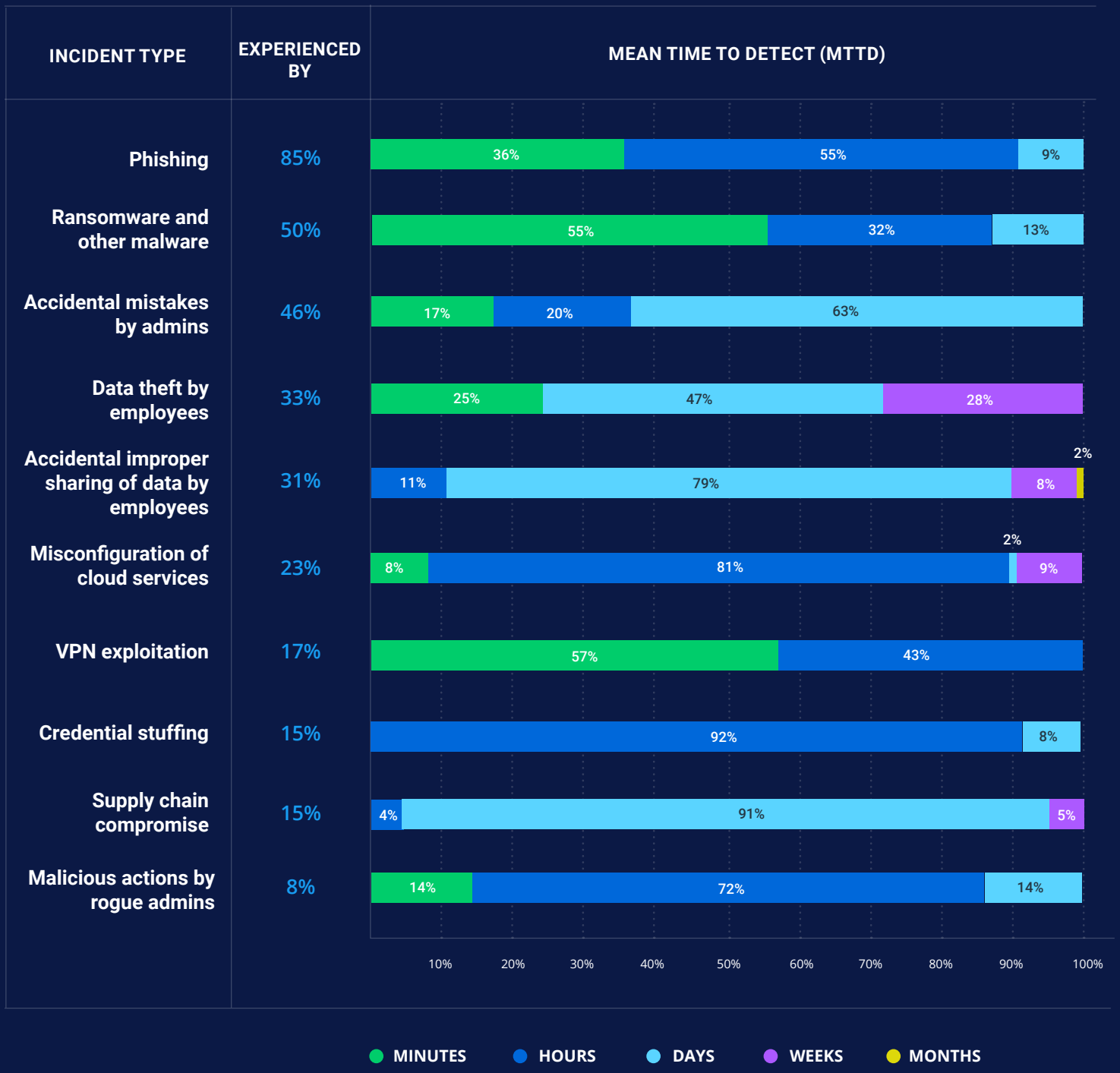
Threats considered critical pre-pandemic and now

MORE ORGANIZATIONS IN FRANCE REPORTED PHISHING THAN THOSE IN OTHER COUNTRIES.

During the first few months of the COVID-19 outbreak, 85% of French organizations experienced phishing attacks, which is higher than any other country analyzed in the survey. What is particularly worrying is that over half of those incidents (55%) remained undetected for hours, which means that attackers could have had enough time to steal sensitive data.

However, the most concerning type of incident in terms of detection was supply chain compromise. Even though relatively few organizations experienced it, almost every one that did admitted it took days to detect it. Such poor detection capability can enable attackers to lurk in the network for a long time, harvesting sensitive data and committing other crimes.

Most common cybersecurity incidents since organizations went remote



THE MOST COMMON SECURITY METRIC USED IS VULNERABILITY STATISTICS.

Nearly two thirds of French organizations regularly report on the state of cybersecurity to their executive leadership teams. The most common metrics they use are incident and vulnerability statistics, followed closely by results of employee training and a general "state of security" score. Only 22% of IT respondents estimate their cybersecurity efforts in financial metrics. 78% say they spend more time on reporting than they should.

64% **of IT professionals in France regularly report on the state of cybersecurity to their executive leadership or board of directors.**

Most common metrics used to report on the state of cybersecurity

Vulnerability statistics	67%
Incident statistics	62%
Results of employee training	59%
A general "state of security" score	56%
Return on investment for security products	22%
Total amount spent on cybersecurity	20%
Total cost of ownership of security products	11%

GERMANY

ORGANIZATIONS ARE WORRIED ABOUT USERS NOT FOLLOWING SECURITY GUIDELINES.

A third of organizations in Germany (34%) believe they are at greater cybersecurity risk now than before the pandemic. Their top concern is that users might ignore security guidelines, though more than half also cited stronger or more frequent cyber attacks.

34% of German organizations are at greater cybersecurity risk than before.

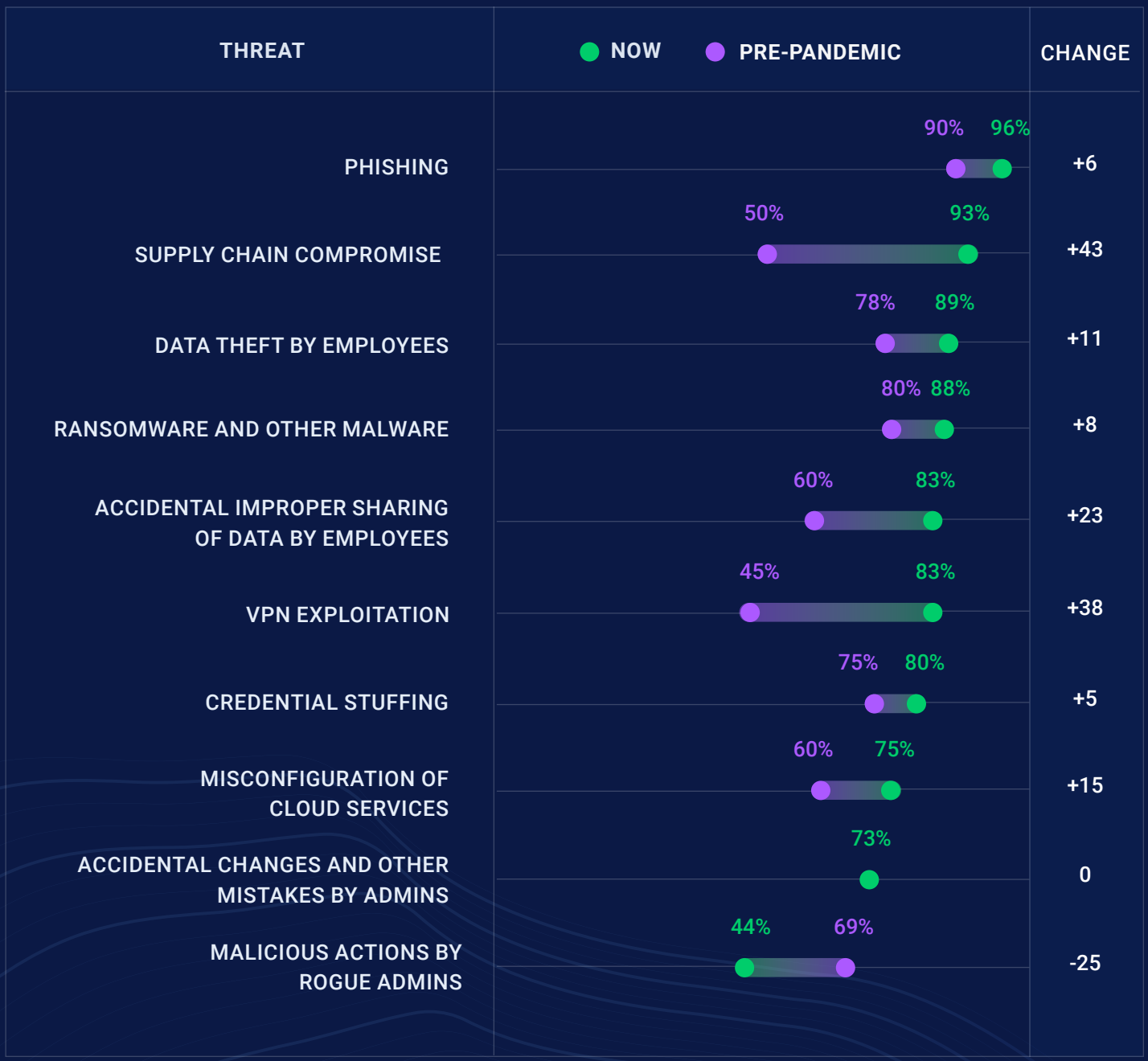
Security concerns of those who feel they are at greater risk

Users may ignore security guidelines	67%
Stronger or more frequent cyber attacks	56%
Unexpected security gaps caused by WFH	44%
Sacrificed security in favor of availability	44%

CONCERN ABOUT SUPPLY CHAIN COMPROMISE AND VPN COMPROMISE HAS SOARED.

Nearly all the threats listed were chosen as a key concern by more than 70% of German organizations. While the most commonly named threat is phishing, this type of threat was high before the COVID-19 outbreak. Second in the list is supply chain compromise, which soared from 50% pre-pandemic to 93% now. Worry about VPN exploitation also nearly doubled, from 45% to 83%. The only threat that dropped was malicious actions by rogue admins, which was named by 69% before the pandemic and 44% now.

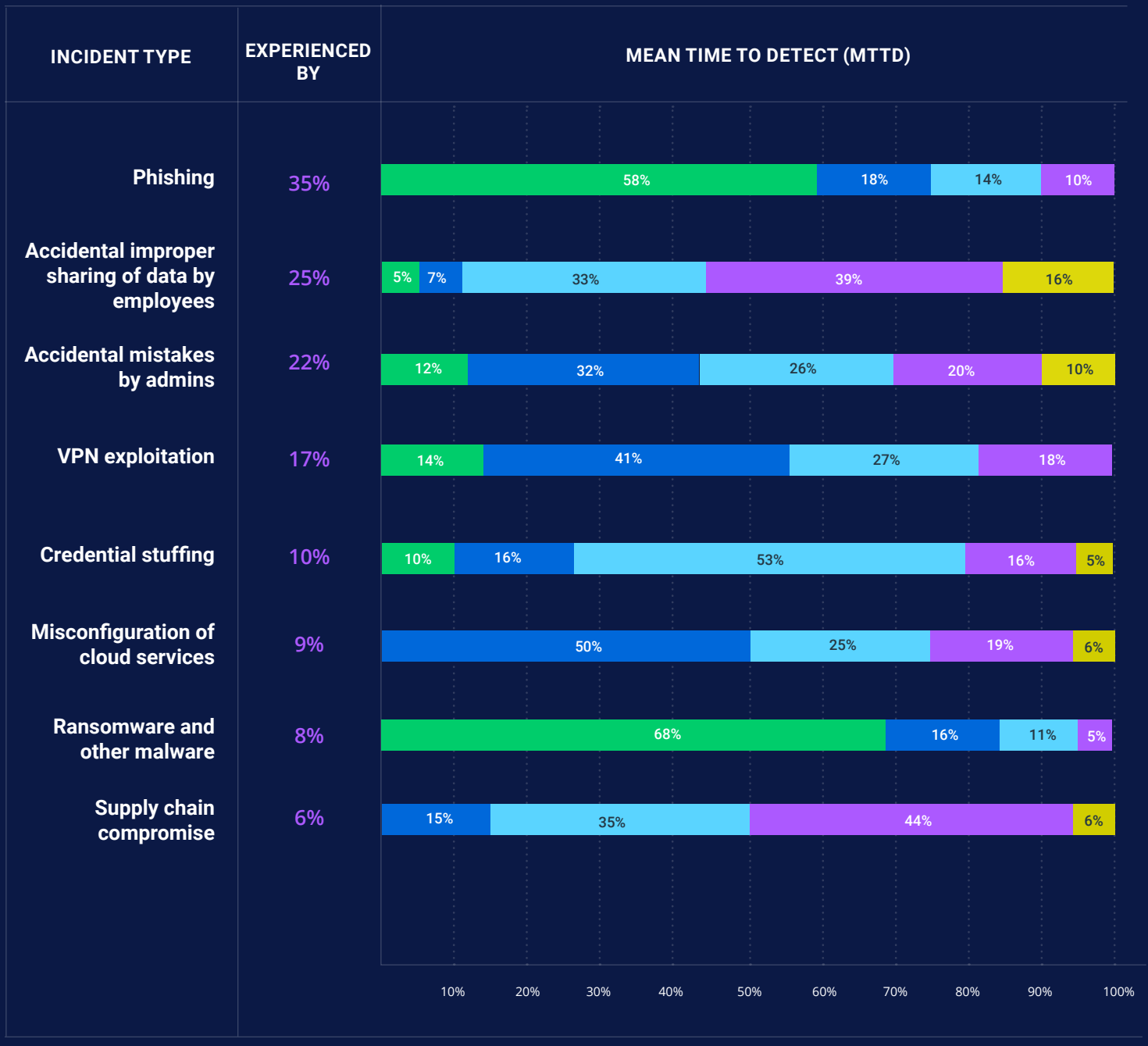
Threats considered critical pre-pandemic and now



INSECURE DATA SHARING IS A COMMON CONCERN, AND THIS INCIDENT IS HARD TO DETECT.

During the past few months, every third German organization suffered a phishing attack; most (58%) of the victims were able to detect it quickly. Insecure data sharing was the second most common incident, and detection took a lot longer: 69% of respondents needed days or weeks, and 16% spent months. Supply chain compromise was also tricky to detect, taking 72% of the victims days or weeks. However, this incident affected only 6% of German IT respondents.

Most common cybersecurity incidents since organizations went remote



HALF OF GERMAN IT TEAMS REGULARLY REPORT ON THE STATE OF CYBERSECURITY TO THEIR EXECUTIVES.

IT teams in every second German organization regularly report on the state of cybersecurity to executives, which is the lowest result for all countries analyzed in this report. The most common metrics that they use are incident statistics (89%) and a general “state of security” score (67%). Only 10% use financial estimations of their security efforts, such as return on investment or total cost of ownership of specific products or tools.

50% **of IT professionals regularly report on the state of cybersecurity to their executive leadership or board of directors.**

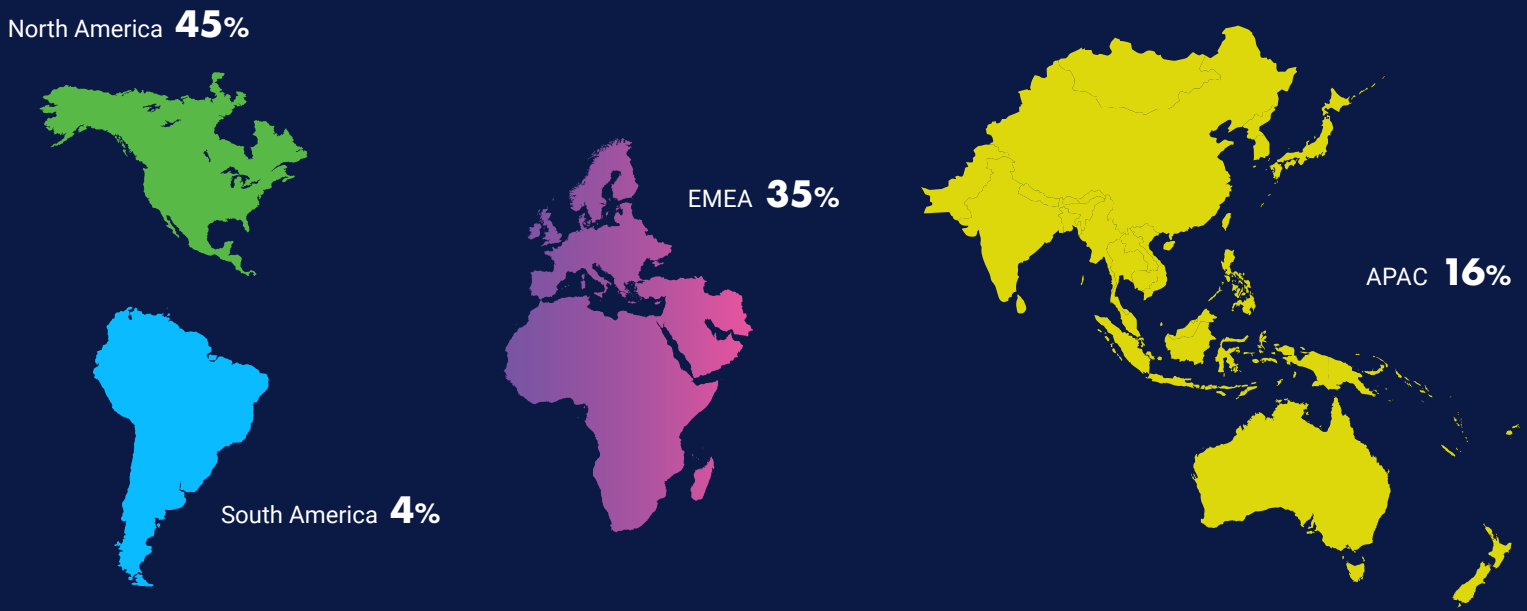
Most common metrics used to report on the state of cybersecurity

Incident statistics	89%
Results of employee training	78%
A general “state of security” score	67%
Vulnerability statistics	65%
Total amount spent on cybersecurity	11%
Return on investment for security products	10%
Total cost of ownership of security products	10%

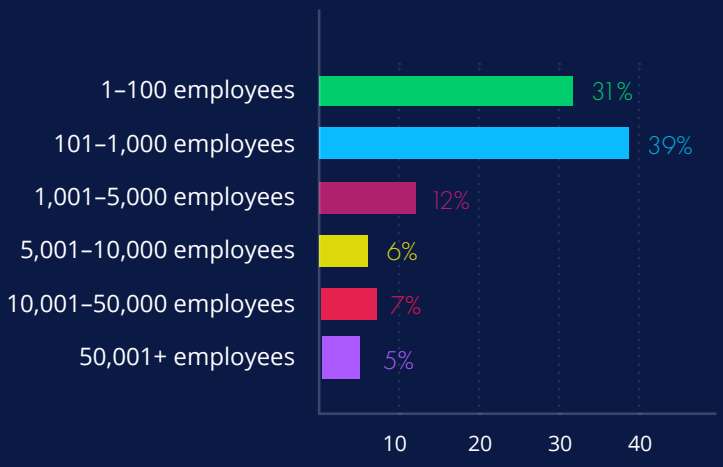
APPENDIX 4:

SURVEY DEMOGRAPHICS

ORGANIZATION LOCATION



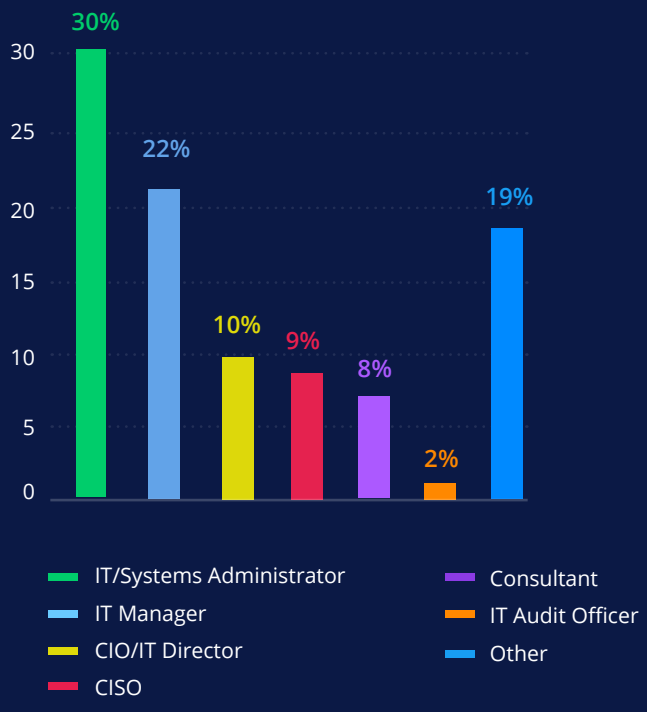
ORGANIZATION SIZE



TOP INDUSTRIES

Technology/Managed Services	11%
Manufacturing	10%
Technology/Software	10%
Banking & Finance	9%
Education	7%
Healthcare	6%
Consulting	6%
Government	6%
Services	5%
Retail & Wholesale	4%
Insurance	3%
Energy	3%
Technology/Hardware	3%
Telecommunications	3%
Entertainment & Leisure	3%
Construction & Engineering	2%

TOP JOB TITLES REPRESENTED



ABOUT THE REPORT

The report is brought to you by Netwrix Research Lab, which conducts industry surveys among IT pros worldwide to discover important changes and trends. For more reports, please visit:

www.netwrix.com/go/research

ABOUT NETWRIX

Netwrix makes data security easy by simplifying how professionals control sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Corporate Headquarters:
300 Spectrum Center Drive, Suite 200, Irvine, CA 92618
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023

www.netwrix.com/social