proofpoint.

REPORT

Europe and the Middle East

2023 State of the Phish

An in-depth exploration of user awareness, vulnerability and resilience

proofpoint.com

A COMMISSIONED SURVEY OF:

7,500

working adults across 15 countries

1,050

IT security professionals across those countries

AND:

135 million

simulated phishing attacks sent by our customers over a 12-month period

18 million

emails reported by our customers' end users over a 12-month period

2022: Cyber Criminals Get Even More Creative

Every year, threat actors look for new ways to outwit victims and bypass defenses. And 2022 was no different. As businesses rolled out new security controls, cyber criminals responded.

They added complex techniques like telephone-oriented attack delivery and MFA bypass. Unknown to most users, these techniques gave cyber attackers a new advantage. And with threat actors constantly upping their game, CISOs and Infosec teams had their work cut out.

Now in its ninth year, our annual *State of the Phish* report explores end-user security awareness, resilience and risk using survey data from 15 countries. The report benchmarks understanding of common cyber attacks and defensive tactics. And then it looks at how gaps in knowledge and cyber hygiene enable the real-world attack landscape. Most attacks target people before they target systems. That's why the final section of this report examines security training practices and outlines opportunities to build and sustain a security-aware culture at every level.

Alongside this year's main report, we've also put together regional summaries to explore how local nuances affect gaps in awareness. This regional summary includes data from **France, Germany, Italy, the Netherlands, Spain, Sweden, the U.K. and the United Arab Emirates (UAE)**. Data has been drawn from surveys of 4,000 working adults and 650 security professionals.

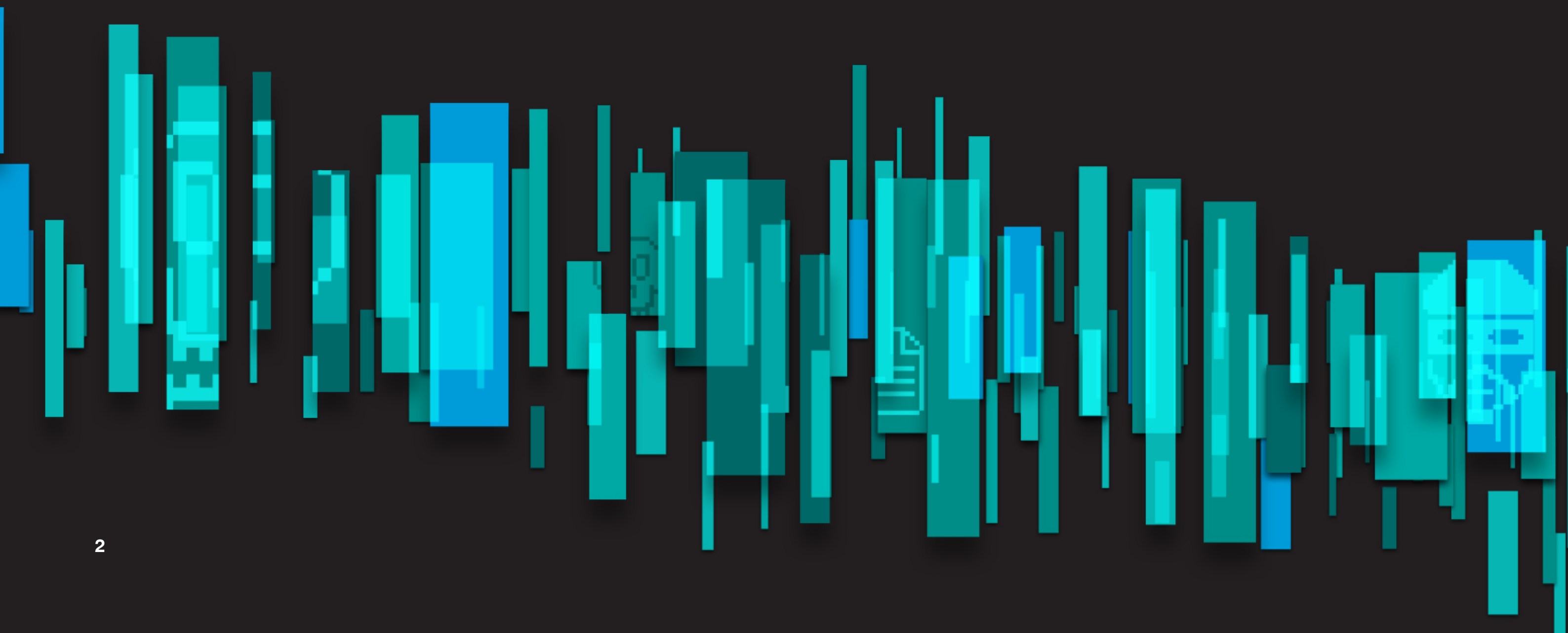
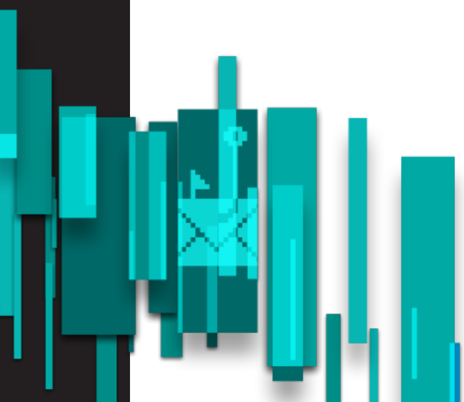


TABLE OF CONTENTS



Key Findings: Global

44%

of people think an email is safe when it contains familiar branding

600K

per day

$300K-400K

telephone-oriented attack delivery attempts daily, with a peak of 600k per day in August 2022

1/3

of people took a risky action (such as clicking links or downloading malware) when faced with an attack

76%

increase in direct financial loss from successful phishing

30 Million

malicious messages sent in 2022 involved Microsoft branding or products

>1 in 10

threats were blocked as a result of user reporting

1/3+

can't define "malware," "phishing" and "ransomware"

Even basic concepts are misunderstood

ONLY 35% of organisations conduct phishing simulations

64% of organisations infected with ransomware paid a ransom

90% of organisations affected by ransomware held a cyber insurance policy

65% of organisations reported at least one incident of insider data-loss

ONLY 56% of organisations with a security awareness program train all their employees

90% of security professionals consider security a top priority at their company

VS.

33% of employees say cybersecurity is not a top priority of theirs at work

94%

of Swedish organisations were likely to suffer a successful phishing attack

but...

Only 18%

of Swedish organisations train their known targeted users

Spotlight on Europe and the Middle East

There were significant variations among all 15 countries surveyed for *State of the Phish*—as you might expect when different languages, cultures and levels of digital maturity are involved. And this also played out among the eight countries in this summary.

Of all the regions that we surveyed, Europe, the Middle East and Africa (EMEA) is arguably the most diverse. Spanning both the northern and southern hemispheres, it's an immense geographic territory that encompasses vastly different cultures, politics and economies. Like many places in 2022, EMEA countries experienced geopolitical changes and heightened conflict. Unsurprisingly, this was reflected in the cybersecurity landscape.

Swedish organisations were the most likely to suffer a successful phishing attack compared to all the countries we surveyed for this report, at 94%. Of course, outlier data could be the result of several factors. One potential explanation is the country's low level of security awareness training—only 18% of Swedish organisations train their known targeted users, which is lower than all other countries. There may also be higher rates of reporting. Sweden has been a pioneer in data security since the 1970s, having passed one of Europe's first digital privacy laws. So, it may be more culturally acceptable to admit to security breaches, leading to more accurate reporting.

This year, we covered Italy for the first time, and the results were surprising. Of all 15 countries, Italian organisations were least likely to experience many types of threat. Only 47% lost data or intellectual property through an external attack (vs. 69% global average). When compared to other countries in this report, Italian organisations were the least likely to be successfully attacked by phishing (79%). These findings may indicate a disconnect or immaturity around security reporting regulations. It could also reflect a culture that is not as focused on transparency and openness of information.

Looking at other cyber attack categories, we noted business email compromise (BEC) attacks are spreading quickly. The Netherlands and Sweden both tied at 92% for the highest rate of attacks (vs. the 75% global average). Incidents rose fastest in Germany and Spain, increasing 16.5% year over year on average. A big factor in the rise of BEC may be its language evolution. Historically, BEC emails have been primarily written in English. Recently, however, we've noticed an increase in BEC in German, Spanish, Slovenian and other languages. This aligns with the increasing sophistication of attacks we're seeing overall.

The Netherlands has the dubious distinction of being the most targeted for cyber attacks by both insiders (86% vs. the 66% global average) and outsiders (84% vs. 68%). But training seems to be effective too. Dutch employees are the least likely to give out personal information or their passwords.

COMING TO TERMS:

Even basic concepts are still not fully understood—more than a third can't define "malware," "phishing" and "ransomware"

40%

of users know what ransomware is, a 9-point jump from 2019—the biggest increase among the terms we asked about

29% and 30%

of users knew the relatively new terms smishing and vishing, respectively

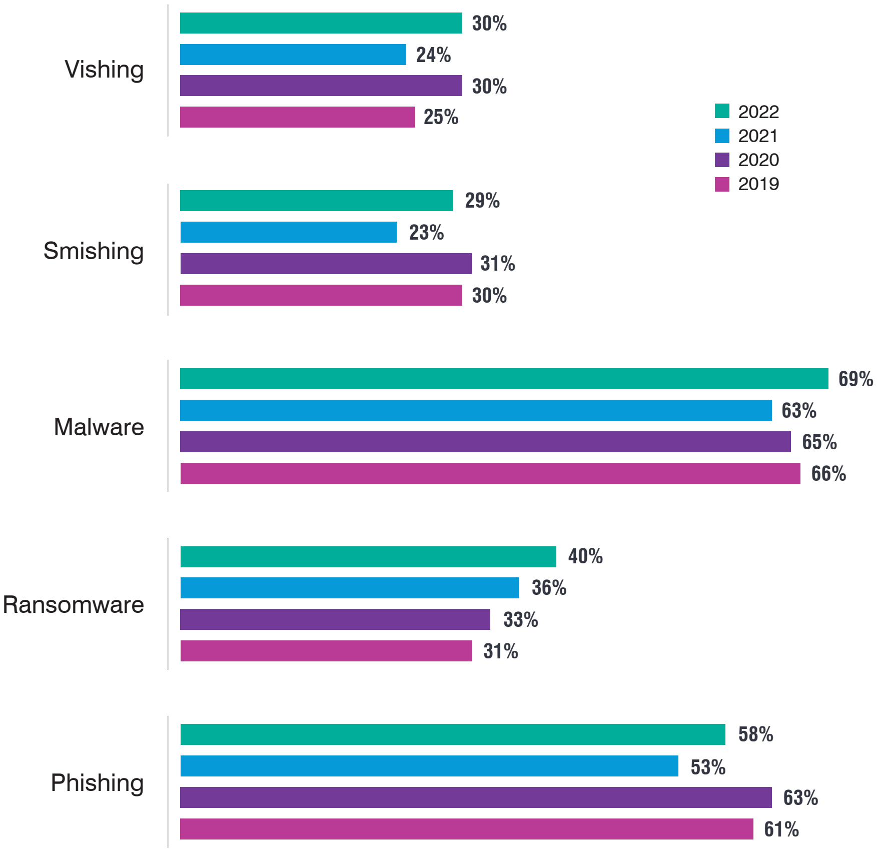
58%

of users knew what phishing is, a 5-point increase from last year but 3 points below 2019

Security awareness: insights and opportunities

Across all 15 countries globally, a similar pattern emerges when we average end-user knowledge of basic security terms. Common threats such as phishing, ransomware and malware have been around for years, but people still don't fully understand what they are. And there is even less awareness of newer threats such as smishing (SMS phishing) and vishing (voice phishing). Disappointingly, our data shows little change year on year.

End-User Understanding Shows Little Change from Year to Year



THE UNCERTAINTY PRINCIPLE:

69%

of users in the Netherlands knew what phishing is, the highest percentage among the eight countries we surveyed in this region

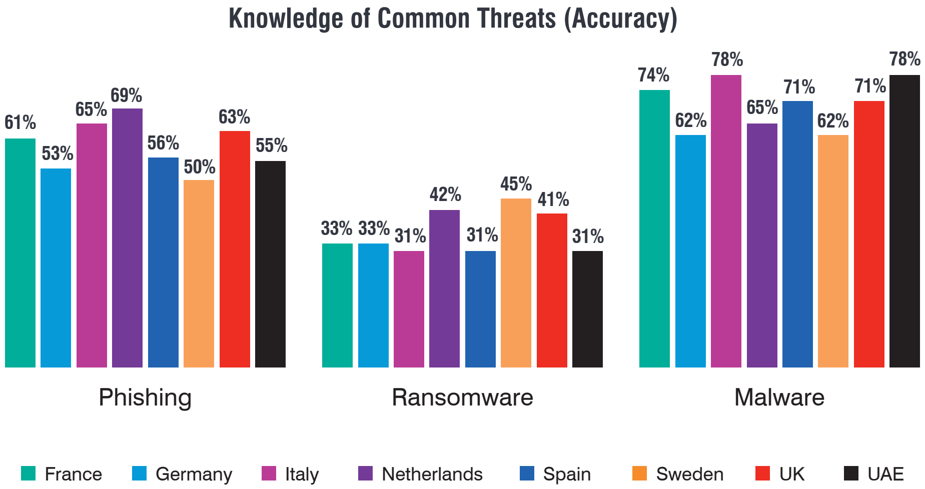
45%

of Swedes were familiar with the concept of ransomware, edging out the other seven countries

78%

of users in Italy and the UAE knew what malware is, the highest rates of awareness among the eight countries in this region

Several notable differences emerge when comparing user knowledge of the three most common threats. Swedish and German respondents were least able to define "malware" or "phishing." In contrast, UAE and Italian respondents were most able to define "malware" but scored lower than average for "ransomware."



These differences could be explained by the fact that less than 50% of European and Middle Eastern organisations train on these topics. Regional averages were 37% for phishing, 34% for ransomware, 40% for malware and 27% for BEC.

TOPICAL TRAINING:

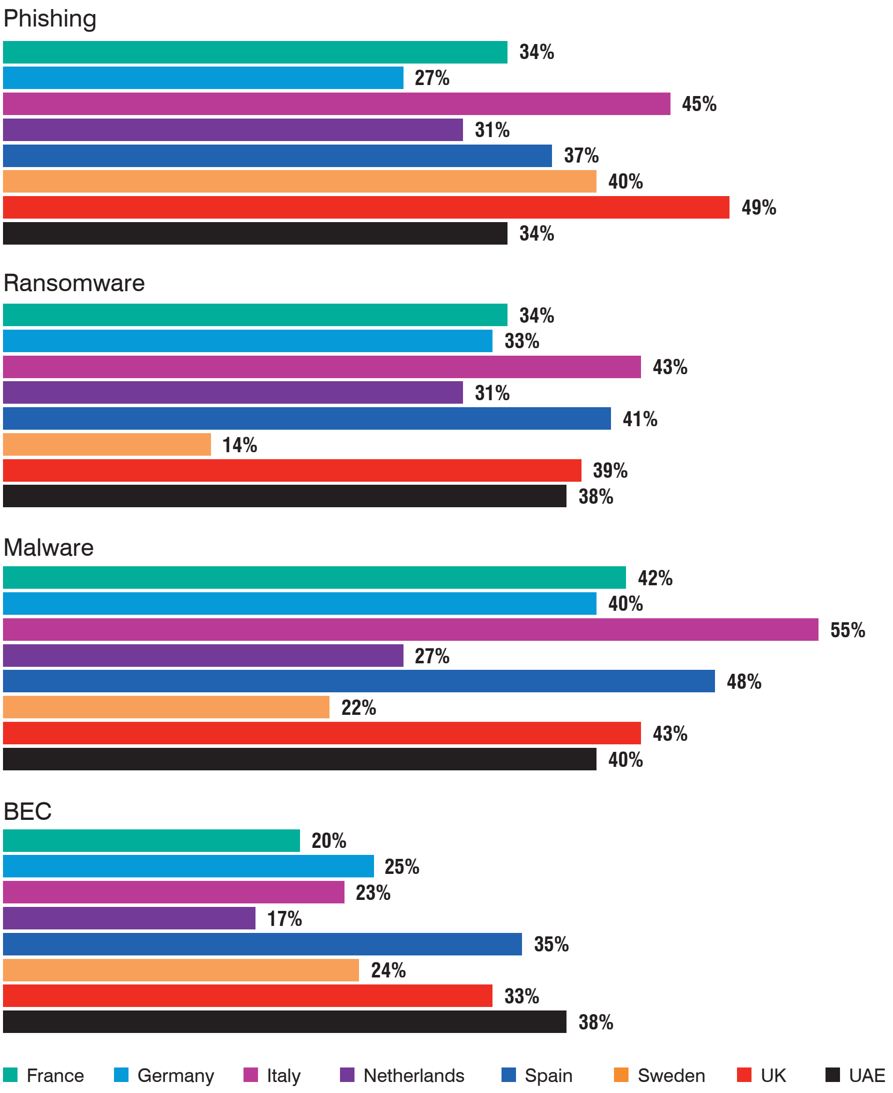
55%

of Italian organisations educate users about malware, the highest percentage of any topic across all of the countries in the region

14%

of Swedish organisations educate users about ransomware, the lowest percentage of any topic across the countries in this region

Threat Topics Coverage in SAT Programs



While most organisations have a security awareness program, not all employees within these organisations receive training. One standout was UAE organisations—64% train all employees and 52% train their known targeted users. Plus, 74% of UAE organisations train employees on security topics that explicitly target their organisation, which is higher than the other 14 countries.

AWARENESS FOR ALL:

64%

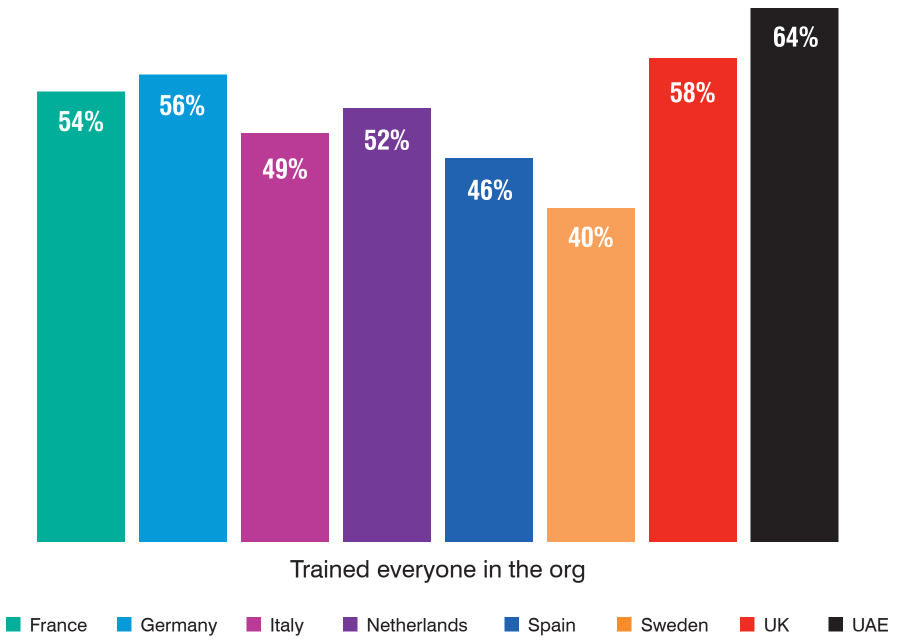
of employers in the UAE trained everyone in their organisation, the highest percentage among the countries we surveyed across Europe and the Middle East

40%

of Swedish organisations did the same, the lowest among the countries surveyed in this region

U.K. CISOs seem to be doing a good job of making security a priority at their organisations. U.K. employees were the most likely to have confidence in their IT team, as well as the most likely to say their organisation makes cybersecurity a priority. Their belief may be down to training—U.K. organisations tied with the UAE for the highest rates of training for known targeted users (52%).

Percentage of Organisations That Trained Everyone in Their Security Awareness Programs



Phishing simulations were most popular in Spain (see charts on next page), at 48%. And the U.K. was notable for placing a high value on the personal touch, with 45% training in person. Within the region, U.K. organisations were the most likely to cover phishing (49%) but were considerably less likely than Spain to use phishing simulations (39%).

TRAINING TYPES:

45%

of U.K. organisations offered in-person training, the highest of any country among European and Middle Eastern countries surveyed

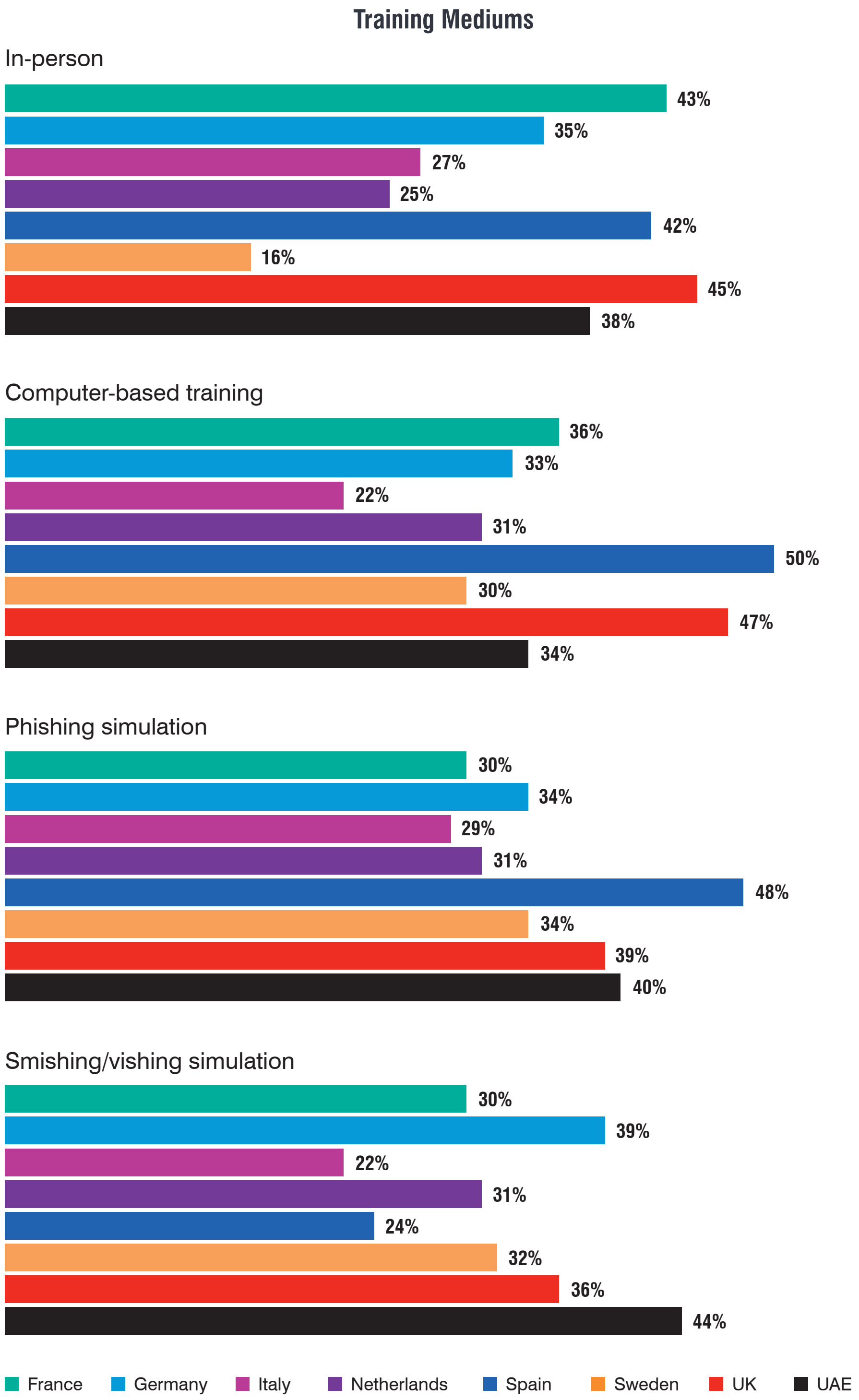
50% and 48%

of Spanish firms offered computer-based training and ran phishing simulations, respectively, making the country a regional standout

44%

of UAE-based organisations ran smishing and vishing simulations, the highest percentage in this region

Training data for Sweden was notable because it suggests organisations may not take security seriously enough. Few organisations do in-person training (16%). They're also the least likely to train everyone (40%). This is surprising considering ransomware infections are higher in Sweden than in any other country surveyed in this report (82%).



THE THREAT WITHIN:

71%

of organisations across EMEA lost data to insiders

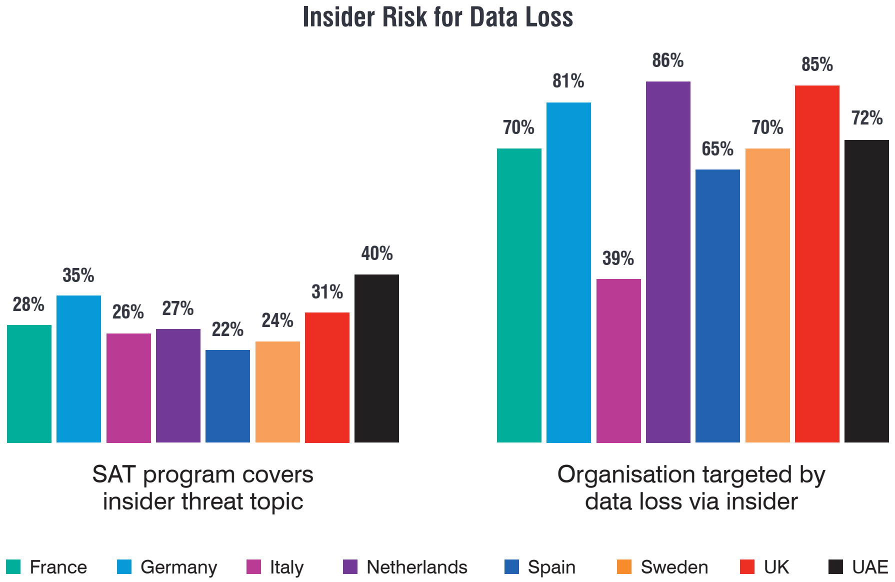
54%

faced three or more attacks

Security awareness: spotlight on insider threats

This year, we expanded our survey to reflect the growing influence of insider threats—a category that extends from malicious data theft to negligent data loss and credential theft.

Across the region, an average of 71% of organisations lost data to insiders. What's notable is the disconnect between the high level of attacks and the low average level of security awareness training, at 29%.



German organisations were most likely to experience frequent insider attacks (18%) And German employees were also the most likely to take work information with them when leaving their job. This may be because German employees simply believe that information belongs to them—only 35% of German organisations train on insider threats. Compare that to UAE organisations—while only 4% report frequent insider attacks, they train employees at a rate of 40%. This may be because UAE employees accidentally hand over personal information or account passwords to people who shouldn't be trusted at the highest rates in the region (29%).

Italian organisations were less likely than other surveyed countries in the region to face targeted attacks across a range of categories.

79%

faced phishing attacks

51%

faced BEC

63%

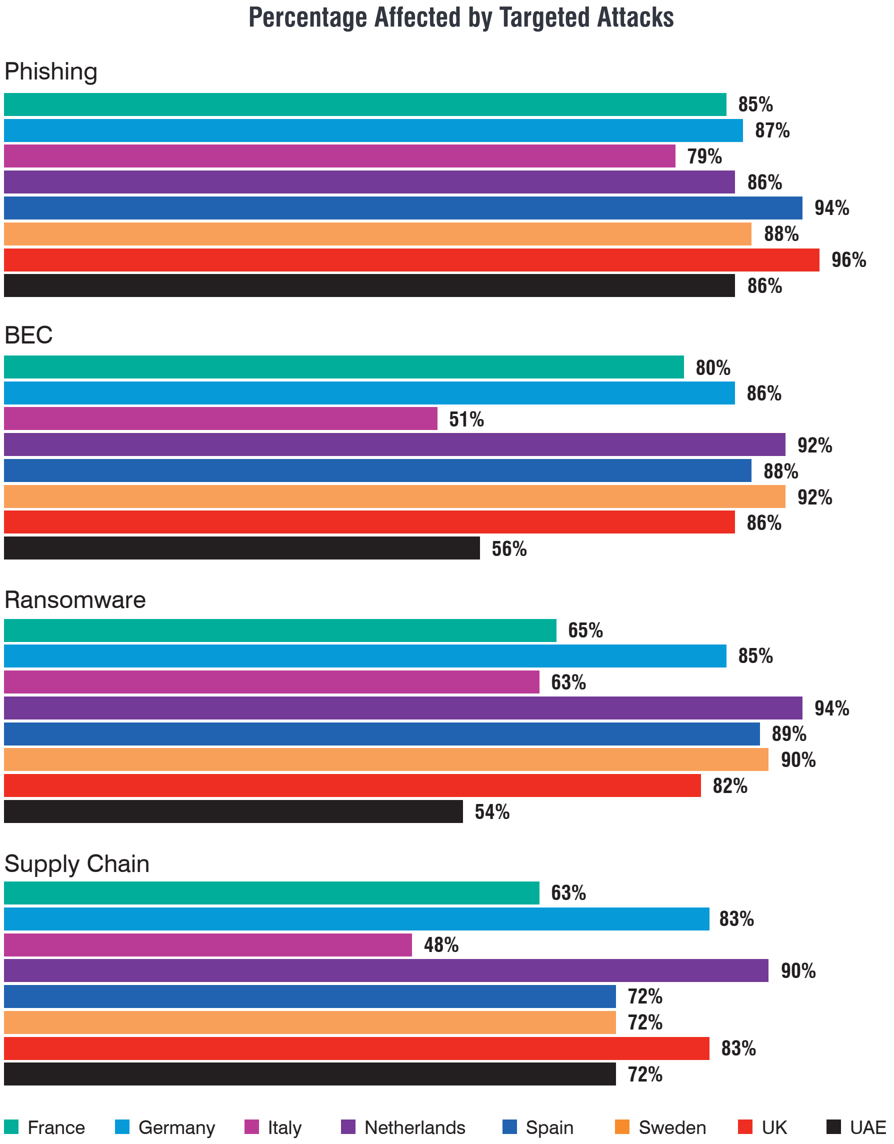
faced ransomware (only the UAE was lower)

48%

faced supply-chain attacks

Threat Landscape Trends

Overall, France was notable for being consistently in the median across the region for falling victim to targeted attacks. We suspect this reflects the country's cybersecurity maturity.



PAYING UP:

27%

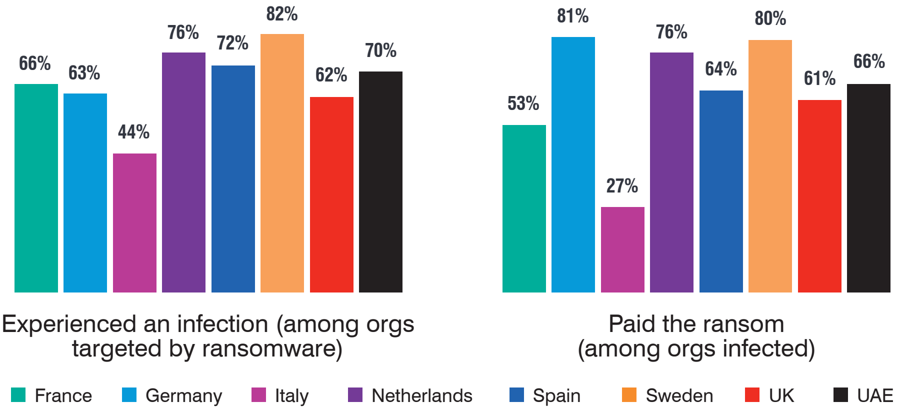
of Italian organisations infected by ransomware paid attackers' ransom demands, the lowest percentage among the countries in this report. Italian organisations were also the least likely to experience an infection in the first place (44%) and the least likely to be reimbursed by their insurer (56%).

Ransomware: insurance lends a hand

Ransomware is a common follow-on attack after initial compromise. Five EMEA countries showed a high probability of ransomware infection.

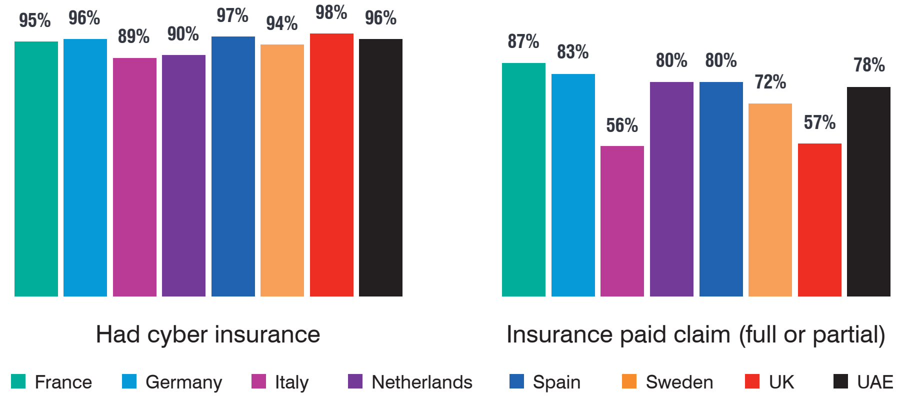
Of all countries surveyed in this report, Sweden was the most likely to be infected with ransomware (82%). As one of the most well-connected countries in the world, Sweden is a front runner in digitisation of both its public sector and core industries. It may be that during the pandemic many organisations were not as careful to protect against cyber threats.

Ransomware Infections and Payments



While German organisations were the more likely pay (81% vs. a 64% global average), U.K. organisations fared worse overall when compared to the other 14 countries. Not only did they fail to get access to their data after payment (33% vs. 52%), but their cyber insurance claims were denied most often (23% vs 7%).

Ransomware Infections and Payments (Among Orgs Infected)



Recommendations

With so much variation between markets and businesses, an individual security program tailored to real-life threats and user risk is the ideal. But if you aren't quite there yet, this year's State of the Phish suggests a few helpful approaches.

Reduce complexity by asking the right questions.

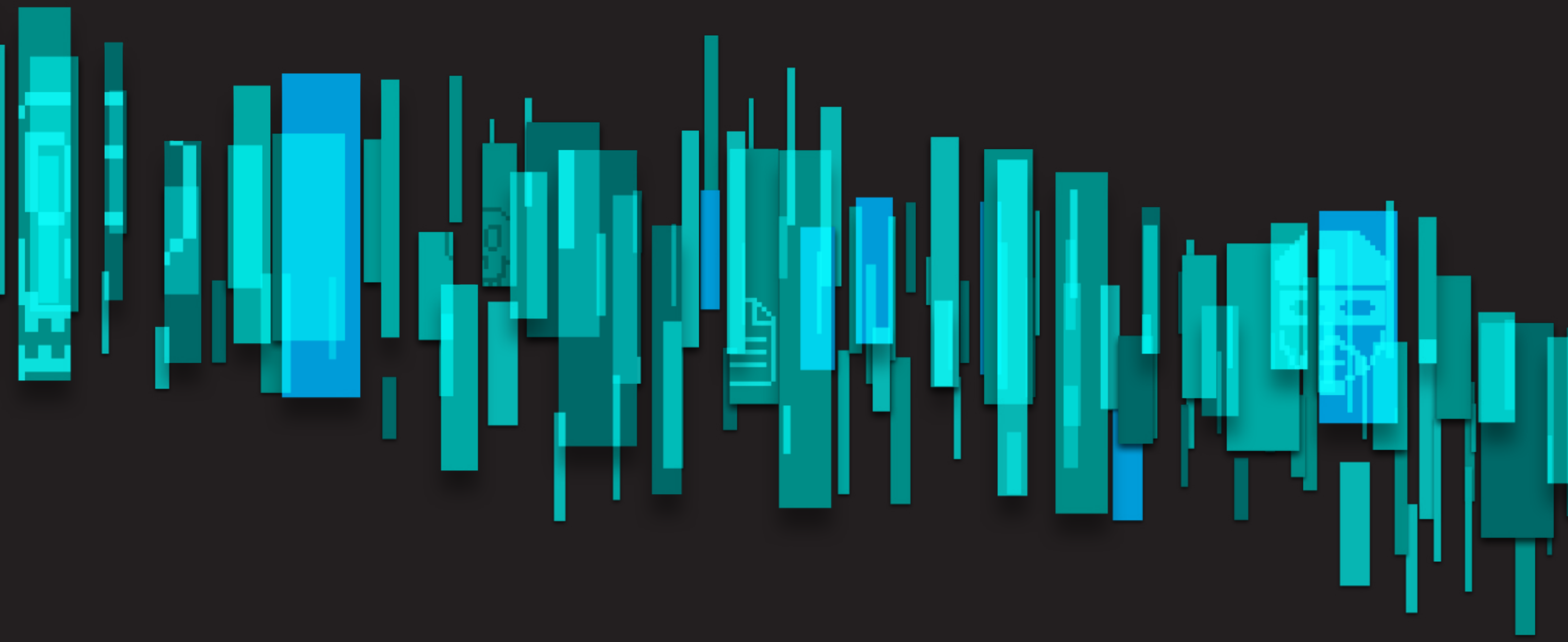
- Who in my organisation is being attacked?
- Where are the current defensive gaps?
- What are my priorities to mitigate human risk?

Pair threat intelligence with organisation-wide security awareness education.

- Identify which users are most likely to be targeted and who is most likely to succumb.
- Match training content to threats currently circulating.
- Train people to recognise phishing using the lures targeting them.

Build a security culture that goes beyond training.

- Training is crucial but not sufficient.
- A strong workplace security culture will encourage users to take information security more seriously in their personal lives.
- Measure the metrics that matter and respond with appropriate and fair remediation.



LEARN MORE

To learn more about how Proofpoint provides insight into your user-based risks and helps you mitigate them with a people-centric cybersecurity strategy, visit **proofpoint.com.**

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**