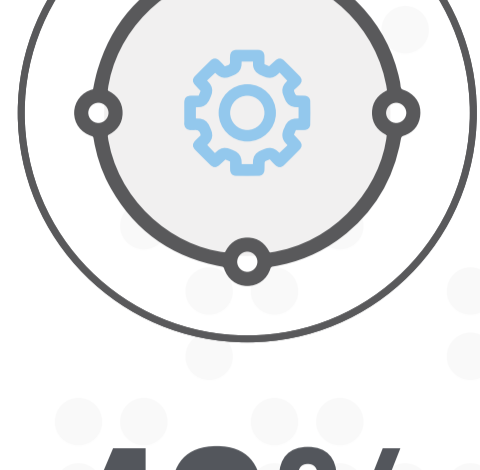


CYBERSECURITY CHALLENGES IN FINANCIAL SERVICES – MARKET SURVEY RESULTS

We asked 250 CISO/CIOs working in large financial service organizations across the world about their cybersecurity challenges in 2020 and beyond. Here's what our research revealed.

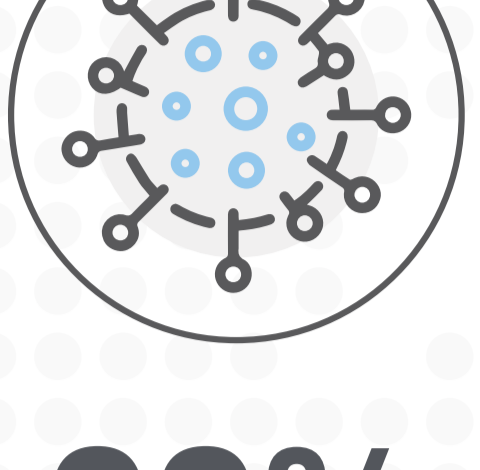
65% OF LARGE FINANCIAL SERVICE ORGANIZATIONS HAVE SUFFERED A CYBERSECURITY ATTACK IN THE LAST 12 MONTHS.

WHAT CYBERSECURITY THREATS HAVE THE POTENTIAL TO CAUSE THE MOST DAMAGE IN THE NEXT YEAR?



46%

Cybersecurity weakness in the supply chain



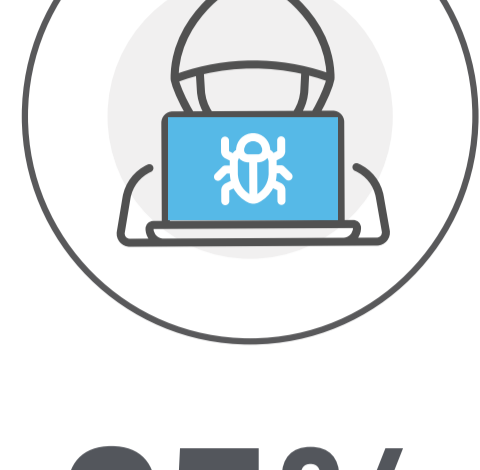
36%

Increased working from home during Covid



35%

Hackers gaining access to our core systems



35%

Insider threat – malicious or accidental



31%

Data breaches



28%

Ransomware attacks

WHAT ARE THE IMPLICATIONS OF A CYBERSECURITY ATTACK OR BREACH THAT FINANCIAL SERVICE ORGANIZATIONS FEAR THE MOST?



51%

Damage to brand reputation



43%

Sensitive customer data being breached



40%

Customer-facing downtime



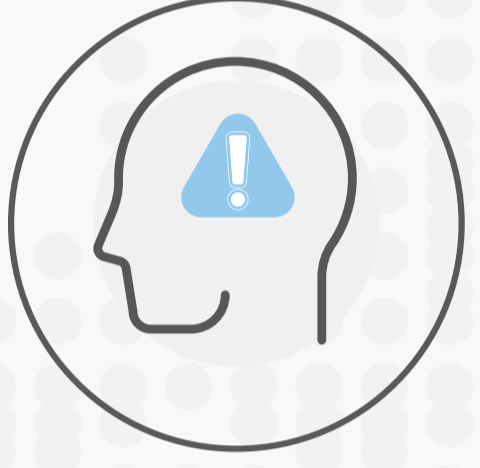
34%

Disruption to internal operations



33%

Loss of access to data caused by ransomware



31%

Loss of intellectual property



30%

Fines from regulatory non-compliance



23%

Loss of customers

92% OF FINANCIAL SERVICE ORGANIZATIONS HAVE INCREASED THEIR CYBERSECURITY SPEND OVER THE PAST 12 MONTHS

WHERE WILL ORGANIZATIONS FOCUS THEIR CYBERSECURITY INVESTMENT IN THE NEXT 12 MONTHS?



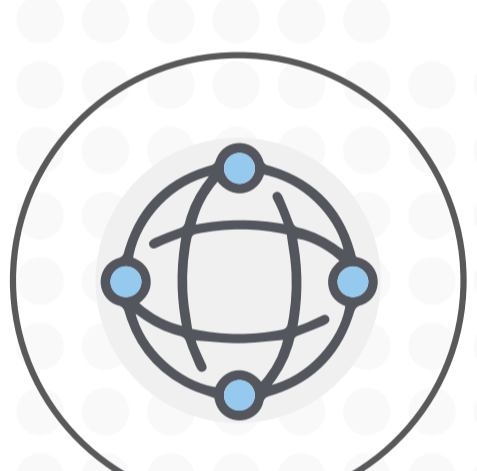
64%

Secure file transfer



63%

Protecting the remote workforce



59%

Networking



56%

Cloud/Microsoft 365



56%

Email security



55%

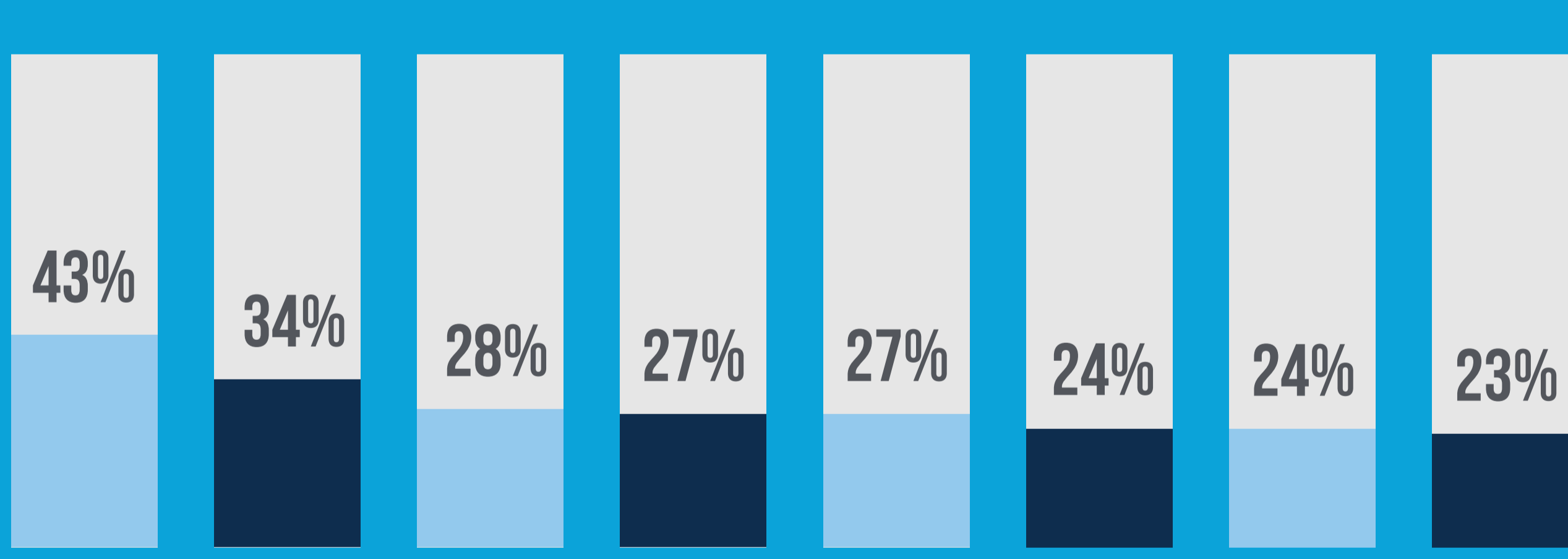
Encryption



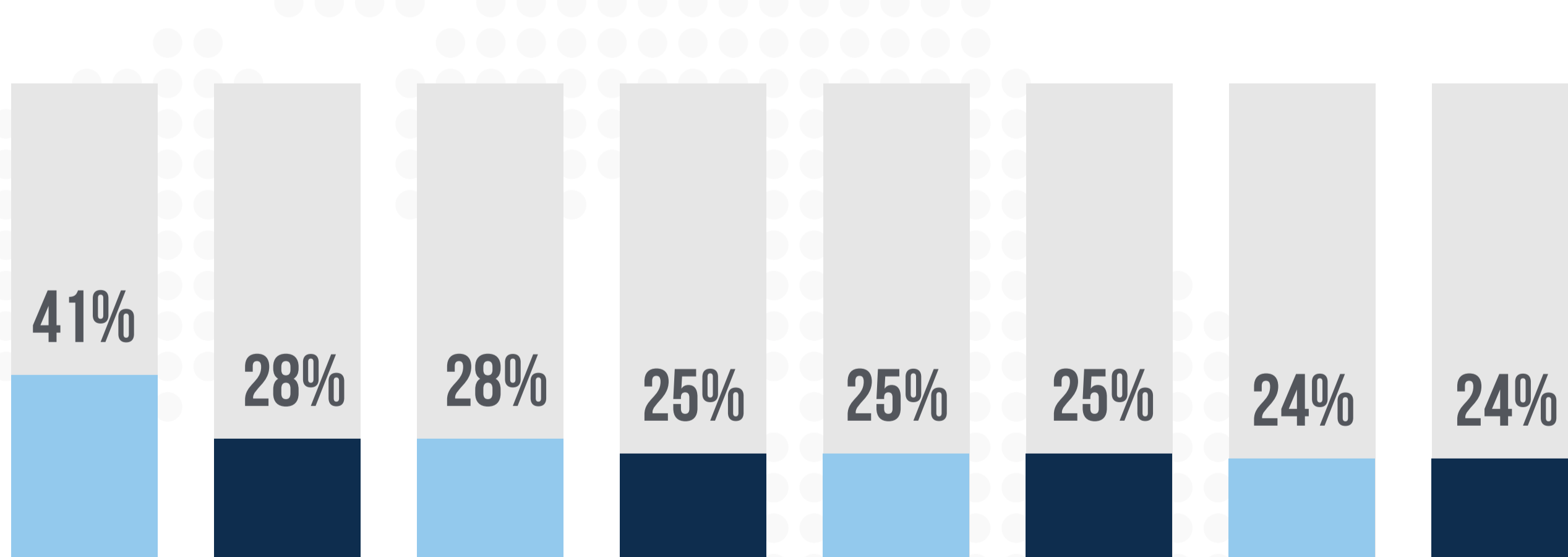
51%

Data loss prevention

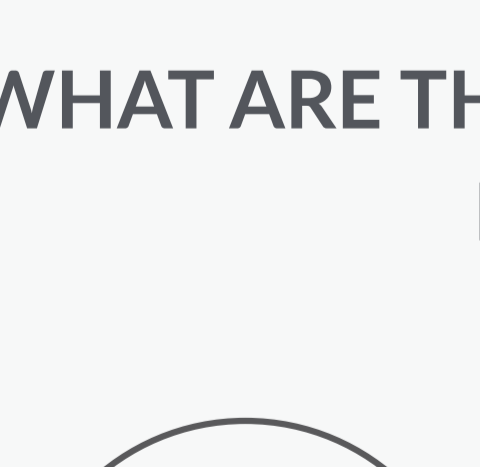
RIGHT NOW, THE MAIN CYBERSECURITY CHALLENGES THE SECTOR FACES ARE:



HOW DO THESE CHALLENGES CHANGE IN THREE YEARS' TIME?



WHAT ARE THE BIGGEST CYBERSECURITY WEAKNESSES CISO/CIOS FACE IN THEIR ORGANIZATIONS TODAY?



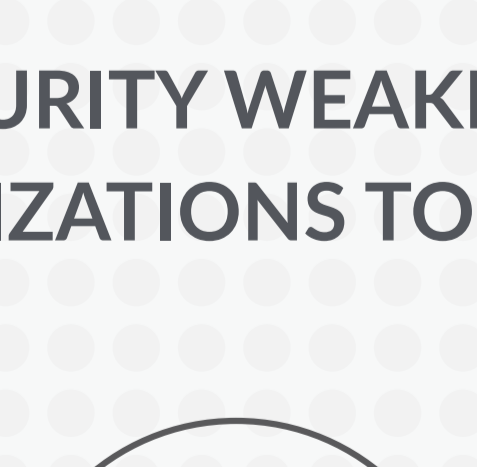
50%

Data visibility



39%

Inability to meet regulatory challenges



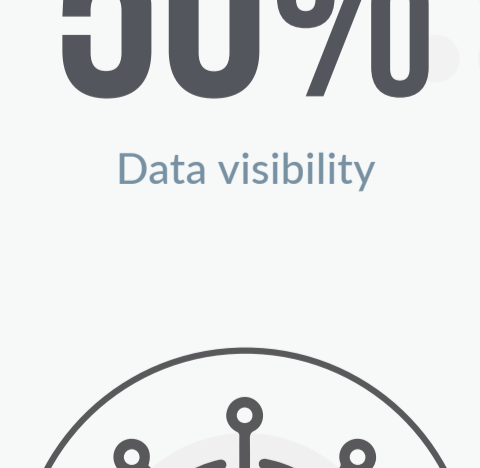
37%

Outdated IT infrastructure



36%

Lack of industry-specific security tools



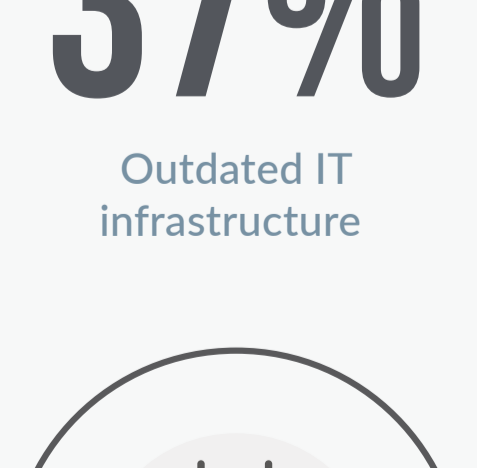
34%

Impact of Covid-19 on cybersecurity and overall business operations



29%

Lack of resources



28%

Lack of budget



25%

Too many manual processes

COVID-19 RELATED CYBERSECURITY CHALLENGES IN FINANCIAL SERVICES

We asked CISO/CIOs working in large financial service organizations across the world about the impact the current pandemic has had on their cybersecurity strategies.

50% | It has increased the need for automation to free up IT staff from manual tasks

45% | We have had to provide more cybersecurity with the same budget, technology, and resources

49% | It has accelerated changes that were already in discussion, such as a move to Microsoft 365

44% | Securing the remote workforce has become a main cybersecurity objective

47% | We have increased investment in secure collaboration tools

36% | Our existing cybersecurity tools were not capable of adapting to the change in working patterns

46% | We had to re-evaluate our cybersecurity training and policies to better reflect the increased home working

35% | We have updated our regulatory best practices

45% | We have noticed more cybersecurity incidents since the increase in home working