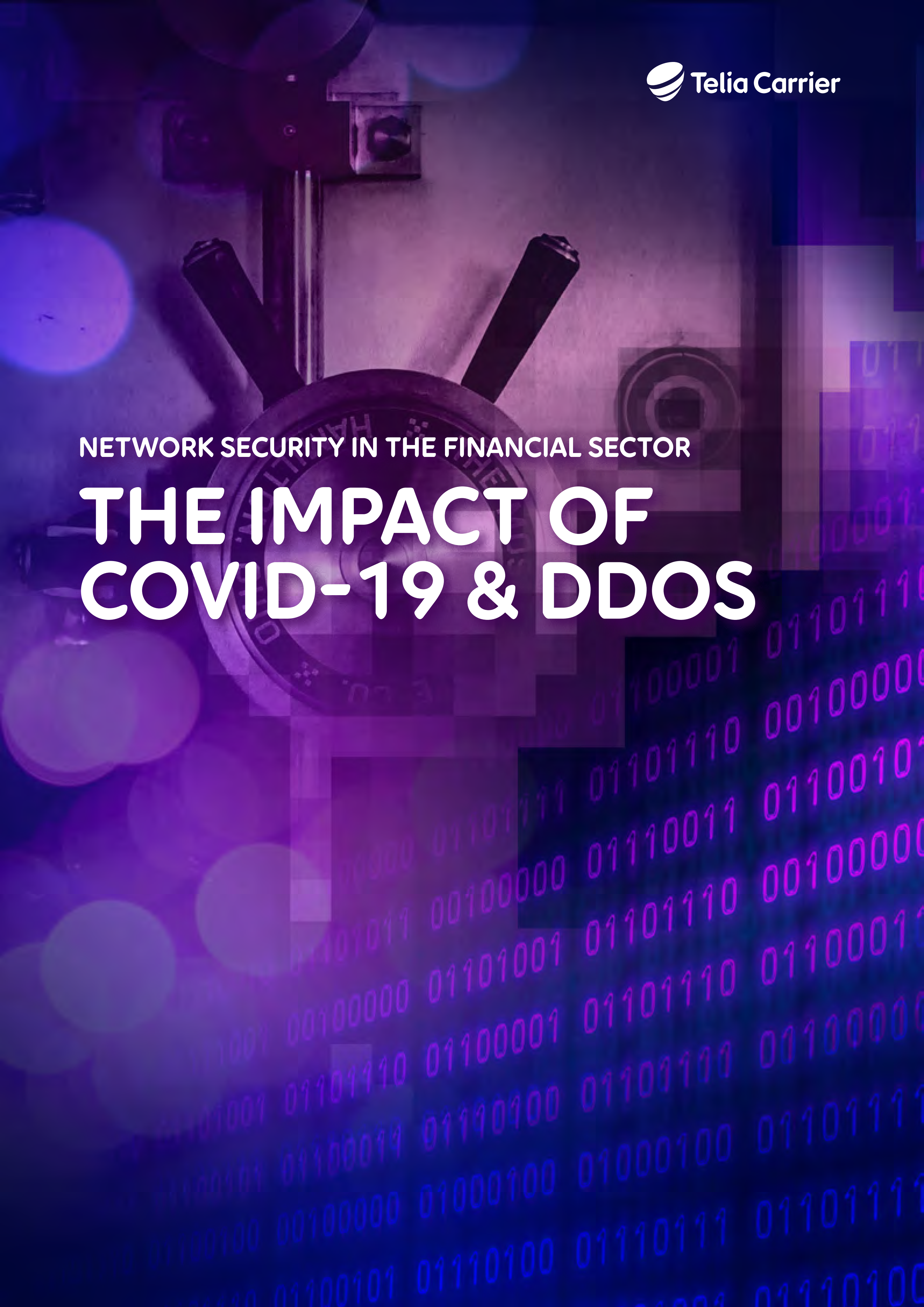


Telia Carrier

NETWORK SECURITY IN THE FINANCIAL SECTOR

THE IMPACT OF COVID-19 & DDOS

HAVE CYBERCRIMINALS BEEN CASHING-IN ON THE PANDEMIC?

Banking and financial services businesses have suffered a huge number of security incidents since the COVID-19 pandemic took hold in March 2020. These include numerous DDoS attacks – often accompanied by ransom demands and extortion. It is therefore unsurprising that 39% of financial sector leaders consider the overall network security threat to be significant.

No doubt, because of the scale of such threats, the cost of securing the network is by far the biggest security outlay that financial sector organisations must absorb.

Covid-19 appears to be a significant driver of change, sparking a sharp increase in security incidents. It seems likely that the wide adoption of remote working practices during the pandemic has enabled cyber criminals to mount opportunistic attacks. In addition, the lockdown presented companies with an unprecedented operational challenge to their IT & communications infrastructure as network management and security teams needed to adapt to remote working. The crisis has left leaders feeling more vulnerable and they are investing more heavily in network security as a result.

These are some of the key findings of recent research into Enterprise Network Security in the financial sector across four of the world's biggest markets – the US, the UK, Germany, and France. The study is based on a survey of senior decision-makers in large banking and financial services companies.

NB. For the purposes of this report, the financial sector (FS) refers to businesses within both the banking and financial services verticals. In places, where banking and financial services merit individual consideration, separate comments and/or statistics are cited.

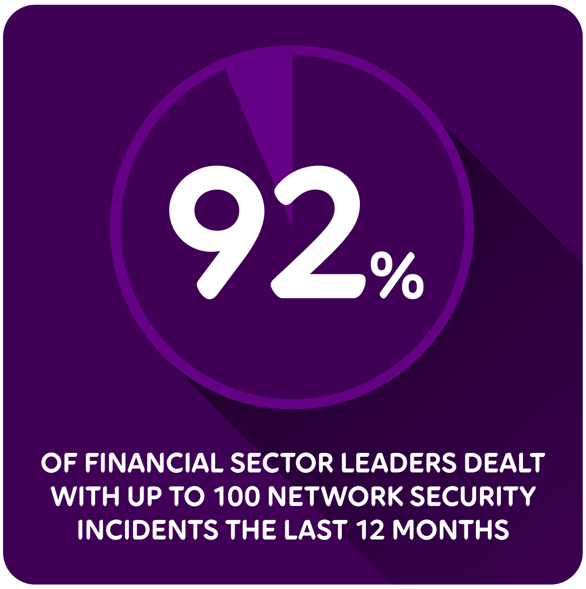
THREATS AND COSTS

NETWORK SECURITY

NETWORK SECURITY INCIDENTS IN THE FS SECTOR ARE STAGGERINGLY HIGH

92% of FS leaders have dealt with up to 100 network security incidents in the last 12 months.

This level of intensity likely reflects the FS sector's inherent appeal to cyber criminals.



OF FINANCIAL SECTOR LEADERS DEALT WITH UP TO 100 NETWORK SECURITY INCIDENTS THE LAST 12 MONTHS

SECURITY THREATS

MANY FINANCIAL SECTOR (FS) LEADERS SEE THE NETWORK AS A SECURITY THREAT TO THEIR BUSINESS

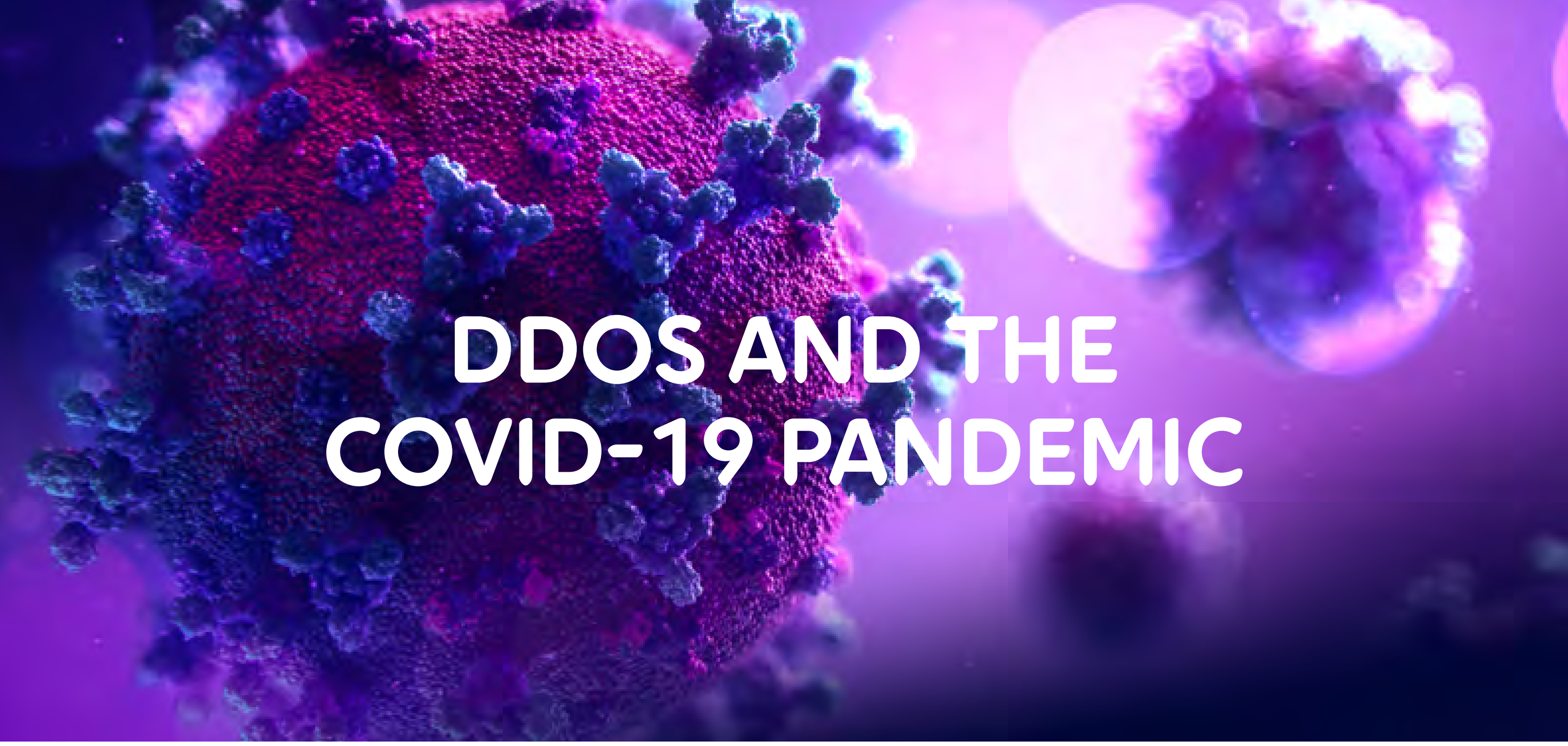
39% of FS leaders consider the overall network security threat to be significant. While systems and applications are a marginally higher concern, this could be because they are a critical component of modern banking and trading platforms.
As a consequence, system downtime, even for seconds, is potentially costly, while longer outages could pose an existential (system-critical) threat.

34% of banking leaders are most likely to be kept awake at night by concerns over logical network security, compared with 23% of financial services leaders.
Worries over physical network security are similarly elevated.

SECURITY COSTS

IN TERMS OF SECURITY COSTS, THE MAIN OUTLAY FOR FS BUSINESSES IS SECURING THE NETWORK

41% of FS leaders see their biggest security costs in the network.
A high level of sensitivity to network security in this sector may account for large sums being spent on it. Does the substantial network cost reflect a need for a greater evaluation of the underlay?



DDOS AND THE COVID-19 PANDEMIC

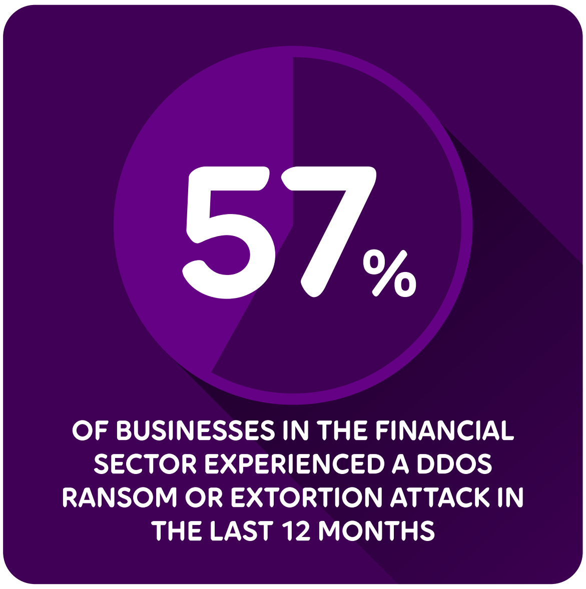
DISTRIBUTED DENIAL OF SERVICE (DDOS)

DDOS ATTACKS ARE HAVING A MAJOR IMPACT

61% **of FS leaders consider phishing to be the main cyber threat to their business**

It could be that access to sensitive data is seen as more important than the security of the infrastructure carrying the data itself. However, it could also be because distributed working provides greater scope for cybercriminals to take advantage of compromised business control processes, allowing them to successfully expedite fraudulent invoices and illegitimate payments.

76% **also perceive DDoS attacks as posing a significant or major threat to their business**



OF BUSINESSES IN THE FINANCIAL SECTOR EXPERIENCED A DDOS RANSOM OR EXTORTION ATTACK IN THE LAST 12 MONTHS

72% **say their company has experienced a DDoS attack in the last 12 months**

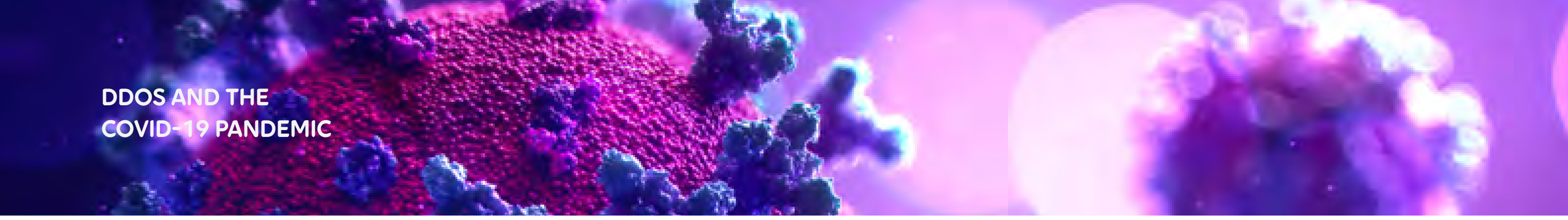
Persistent low-intensity and sporadic high-intensity attacks constitute an equally serious threat.

57% **say that they have experienced a DDoS ransom or extortion attack in the last 12 months**

Such attacks were more common in financial services, where a sizeable 67% had been targeted, compared with 46% of banking organizations.

14% **say that DDoS attacks have posed such a serious threat that they could have undermined their business's ability to continue**

Are FS leaders sufficiently prepared for – and well-protected against – DDoS attacks?



SECURITY EFFECTS OF COVID-19

THE COVID-19 PANDEMIC HAS SEEN A SHARP INCREASE IN SECURITY INCIDENTS, LEAVING LEADERS FEELING MORE VULNERABLE AND INVESTING MORE HEAVILY IN NETWORK SECURITY

58% of financial services companies, compared with 38% of banking organizations, have experienced more security incidents during the Covid-19 pandemic

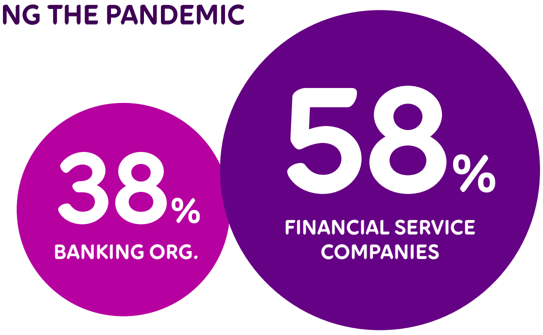
suggesting that financial services companies have been a greater target.

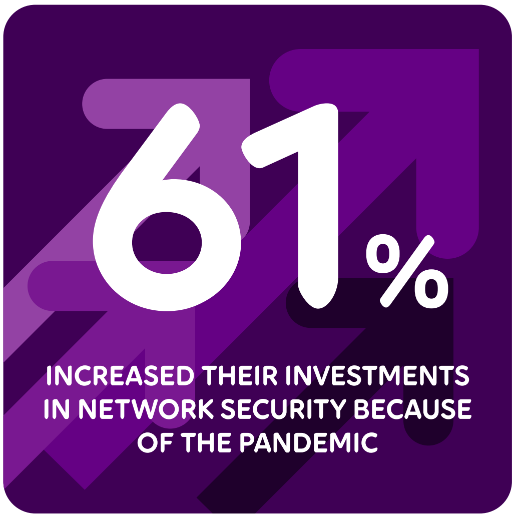
48% of FS leaders feel more vulnerable to security threats

61% have increased their investment in network security because of the pandemic

This is undoubtedly a response to both perceived and actual threats.

MORE SECURITY INCIDENTS DURING THE PANDEMIC





INCREASED THEIR INVESTMENTS IN NETWORK SECURITY BECAUSE OF THE PANDEMIC

WITHIN THE TELIA CARRIER BACKBONE, WE SAW A STAGGERING INCREASE IN DDOS ACTIVITY DURING 2020

There was a 50% increase in peak attack traffic compared to 2019, with a jump to 1.18 Terabytes per Second (TBPS) or 887 Mega Packets per Second (Mpps).

> *"The volume and frequency of DDoS attacks continues to increase, and cyber criminals are using the huge bandwidth available across the Internet to target their victims with speed and ferocity from multiple launch points simultaneously."*

JORG DEKKER
HEAD OF INTERNET SERVICES
TELIA CARRIER

SECURING THE NETWORK

NETWORK UNDERLAY SECURITY

FS LEADERS SHOULD TAKE THE SECURITY OF A SERVICE PROVIDER'S NETWORK UNDERLAY MORE SERIOUSLY

58% of FS leaders don't appear to be making a careful evaluation of the security of a service provider's network underlay in their overall assessment of new services

This figure leaves significant room for improvement, as FS businesses have more reason than most to worry about breaches of network security.

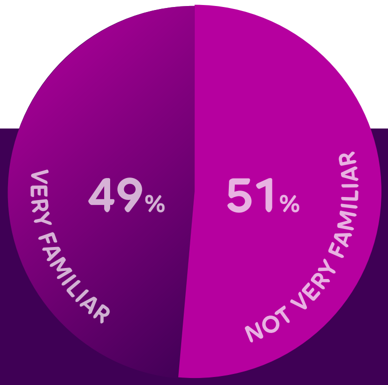
DDOS PROTECTION

THE FS SECTOR COULD BE MISSING OUT ON A COMPELLING OPPORTUNITY TO PROTECT ITSELF BETTER FROM DDOS ATTACKS

49% Only half of FS leaders consider themselves very familiar with the DDoS protection capabilities of their network service provider, with 35% admitting to being only somewhat familiar

52% fail to take advantage of their ISP/network provider's DDoS protection service. Is this a missed opportunity?

40% of banking and 21% of financial services organizations rely on their own mitigation/scrubbing capabilities



ONLY HALF OF FINANCIAL SECTOR LEADERS CONSIDER THEMSELVES VERY FAMILIAR WITH THE DDOS PROTECTION CAPABILITIES OF THEIR NETWORK SERVICE PROVIDER

IMPLICATIONS FOR FINANCIAL SECTOR LEADERS

The research implies that FS leaders should take account of several key issues when considering enterprise and network security.

While greater investment in cyber security is clearly important, ‘throwing money’ at the issue is not a solution in itself. It is critical that FS leaders maintain an accurate and up-to-date picture of the threat landscape and target security investments where they are most needed.

FS enterprises need to evaluate potential security threats throughout their entire ICT ecosystem to combat the growing severity and unpredictability of evolving threats in an increasingly digitalized (and distributed) business environment.

In seeking protection, FS leaders cannot afford to overlook the risks faced in their core network and should give careful consideration to their choice of network service provider.

FINANCIAL SECTOR LEADERS NEED TO CONSIDER:

THE LESSONS OF THE COVID-19 PANDEMIC

– when scaling up their security programs, to take account of the constantly evolving (and unpredictable) nature of threats.

BUSINESS-SPECIFIC THREATS

– how are cybercriminals specifically targeting banking and financial services businesses and where should the focus on mitigation be?

THE GEOGRAPHICAL THREAT LANDSCAPE

– what are the main threats and vulnerabilities within the geographies in which they operate?

LOGICAL NETWORK SECURITY ACROSS THE ECOSYSTEM

– do potential suppliers take a robust enough approach to routing security and security within their network production environment?

THE PHYSICAL SECURITY OF THEIR OWN NETWORKS (AND POTENTIAL SUPPLIERS) AND THAT OF SUPPLIERS PROVIDING UNDERLAY

– businesses need to look beyond logical connectivity and demand full transparency from their suppliers regarding the resilience of physical network assets throughout the extended supply chain – including their hardware vendors and data center partners. They must ensure that their network providers have full visibility (and control) of the underlying network infrastructure.

ALL AVAILABLE DDOS PROTECTION OPTIONS

– what are the different services available to banking and financial services enterprises, and which ones afford the best protection for their specific needs? FS businesses might be missing out on an effective and efficient opportunity to mitigate DDoS if they overlook network provider mitigation options.

RESEARCH METHODOLOGY

This paper is based on an online survey of 131 financial sector decision-makers (79 in banking and 52 in financial services), which was carried out in the US, UK, Germany, and France in the first half of 2021.

It provides insights into current corporate security concerns – from the top of business. All survey respondents are leaders in the financial sector, that is, all are involved in decision-making regarding their company's network security and development strategy. All work for companies employing more than 4,000 people.

The survey was conducted on behalf of Telia Carrier by Savanta, a global leader in digital data collection, and was part of a larger pan-industry survey. A more detailed report, based on the full survey, can be downloaded here:

https://www.teliacarrier.com/knowledge-hub/white-papers/enterprise-security-report-2021.html

ABOUT TELIA CARRIER

Telia Carrier solves global connectivity challenges for multinational enterprises whose businesses rely on digital infrastructure. On top of the world's Number-1-ranked IP backbone and a unique ecosystem of cloud and network service providers, we provide an award-winning customer experience to customers in more than 125 countries worldwide.

Our global Internet services connect more than 700 cloud, security and content providers with low latency. For urther resilience, our private Cloud Connect service connects directly to Amazon Web Services, Microsot Azure, Google Cloud, IBM Cloud and Oracle cloud across North America, Europe and Asia.

teliacarrier.com/knowledge-hub

teliacarrier.com