State of the Market:

The New Threat Landscape

Pushing MSP security to the next level

N-ABLE™

An Independent Report Commissioned by N-able

Adapting to a changing environment

IT managed services providers (MSPs) have faced extraordinary challenges during the pandemic. In many cases, they have carried the burden of responsibility for ensuring their customers have been able to continue to operate in the face of an uncertain and constantly changing business environment. At the same time, they have also had to adapt in order to continue to operate and survive.

Cybercriminals were quick to see this as an opportunity, and there has been a surge in cyberattacks since the beginning of the pandemic. MSPs have increasingly found themselves prime targets for these attacks as cybercrime gangs have looked to exploit their relationships with customers to infiltrate systems and harvest sensitive data.

In response to this changing environment, N-able has launched a benchmarked annual report (in association with Coleman Parkes Research), looking at the role of MSPs and the critical part they play in protecting their customers' businesses. It will also look at how MSPs are being affected directly by security threats, the cybersecurity trends they really need to know about, and what they should be focusing on when it comes to implementing the necessary cybertechnologies to keep both their and their customers' businesses safe.

The reality is that whatever sector you're in, businesses aren't just businesses anymore—they're essential parts of the global infrastructure and supply chain. That makes us all targets. And we're in this together.

EXECUTIVE SUMMARY OF FINDINGS FROM THE REPORT:[1]

- MSPs are fast becoming primary targets for cyberattacks
- Almost all MSPs have suffered a successful cyberattack in the past 18 months, and 90% have seen an increase in attacks since the pandemic started
- 82% of MSPs' customers have seen an increase in attempted cyberattacks
- MSPs are raising security budgets by an average of just 5%—but questions remain as to whether this is enough
- Automating key functions is critical to making headway against cybercriminals
- While backup is a core offering, only 40% of MSPs are backing up workstations every 48 hours or less—this needs to improve
- With just 40% implementing two-factor authentication (2FA) on their own systems, MSPs still need to focus more on implementing the basics
- Small and medium-sized enterprise (SME) security budgets are increasing—giving MSPs an opportunity to sell more and better services

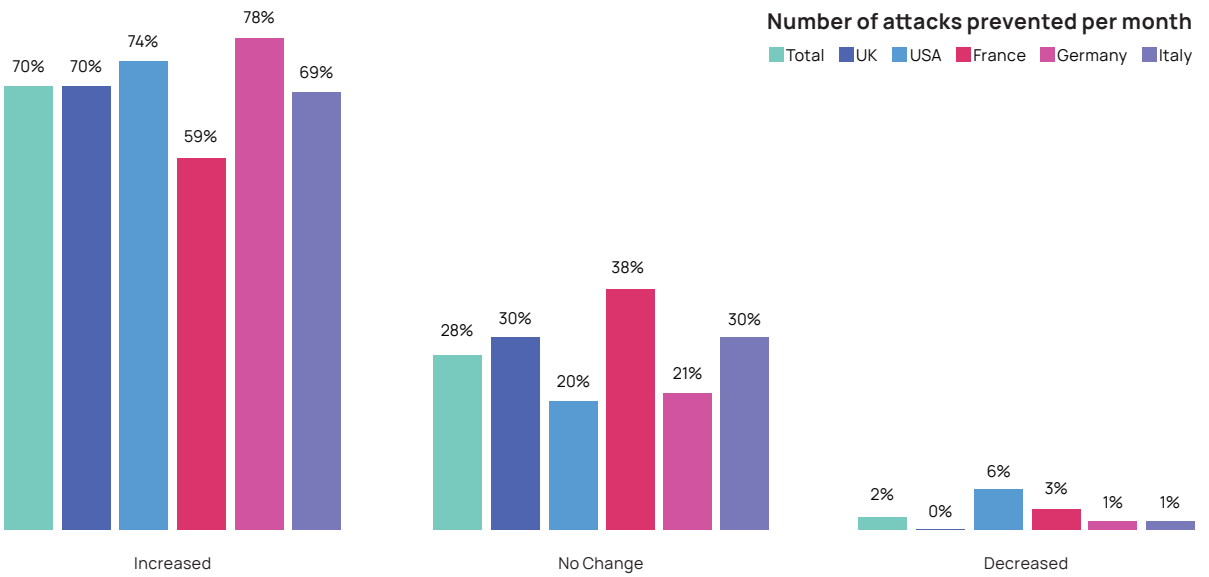
[1]All statistics in this document are based on the fidings of independent research commissioned by N-able.

SMEs are increasing their security budgets

Before considering how their security strategy should change, MSPs need to know one fundamental fact: how will their customers pay for it? Many businesses have been through an incredibly tough couple of years, and while we know the importance of improved security, it may be a tough sell for many SMEs right now.

There's good news. According to our report, the majority of SMEs, 7 in every 10, are planning to increase their security budget. The one outlier is France, but even there, 6 in 10 SMEs are increasing their budgets.

Of the rest, most are maintaining the same budgets, with only 2% looking to decrease budgets. The increases are substantial, an average of 7%. Given recent circumstances, this is a solid investment by businesses in security.



For MSPs, this means there is a big opportunity available. For many customers, they do not have to work hard to convince them that security is important and needs investment; rather, the conversation needs to be about where the money should be spent and how to make the most of this increase.

SMEs are keen to spend this increase on data security and cloud security, with identity access way down the priority list. MSPs should follow their customers' lead to an extent when offering additional and improved services, but should also remember that they are the expert.

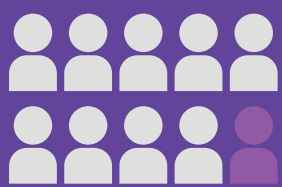
- Data security
- Cloud security
- Infrastructure protection
- Security services
- Network security equipment
- Application security
- Integrated risk security
- Identity access security

Attacks on MSPs are on the rise

Cyberattacks are almost constantly in the headlines today. We have seen massive ransomware attacks cripple supply chains and utilities services across the globe.

MSPs have long been viewed as a potential attack vector. They provide a convenient entry point into the supply chain, which allows cybercriminals to compromise their systems and get access to customers' sensitive data and systems. Their significance has been greatly elevated in the eyes of threat actors thanks to the effects of the pandemic and the ability to weaponize their remote monitoring and management (RMM) software to conduct a variety of attacks, including business email compromise (BEC) and ransomware attacks. This is a change in focus for the bad guys that is likely here to stay.

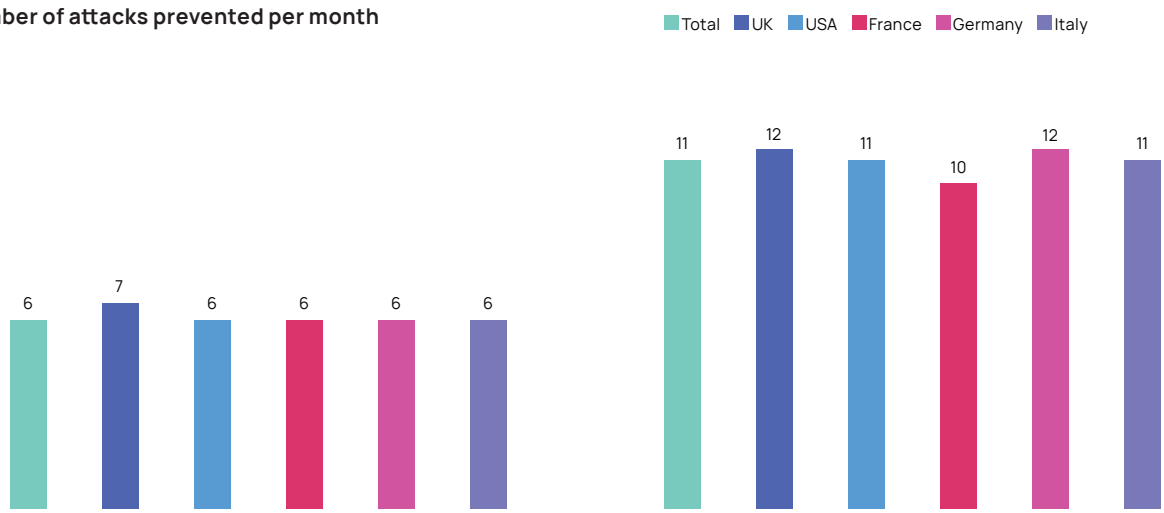
One reason why MSPs continue to be seen as an attack vector is that far too many attacks are successful. Our report found that almost all MSPs have suffered a successful cyberattack in the past 18 months. And 90% have seen an increase in the number of attacks since the start of the pandemic. On top of this, a third have been successfully attacked in the last quarter alone. It's also important to note that the number of attacks these MSPs are preventing has almost doubled, from 6 to 11.



9/10 people

90% have seen an increase in the number of attacks since the start of the pandemic.

Number of attacks prevented per month



Average number of attacks per month **BEFORE** the pandemic

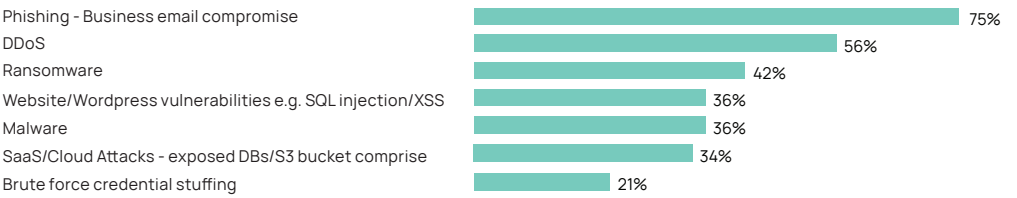
Average number of attacks per month **SINCE** the pandemic

Single code per option

Base: Respondents experiencing an increase in cyberattacks (451) UK(86) USA(85) France(92) Germany(90) Italy(98)

Understanding attacks and attack vectors

Type of attacks targeted most frequently



The MSPs we surveyed reported seeing attacks proliferate in three key areas (with some regional variation):

1. PHISHING

Phishing is the most common attack vector, with Italy (86%) and France (82%) experiencing the most attacks in this area.

2. DDOS

DDoS is an increasingly popular attack vector in the U.S., at 65%.

3. RANSOMWARE

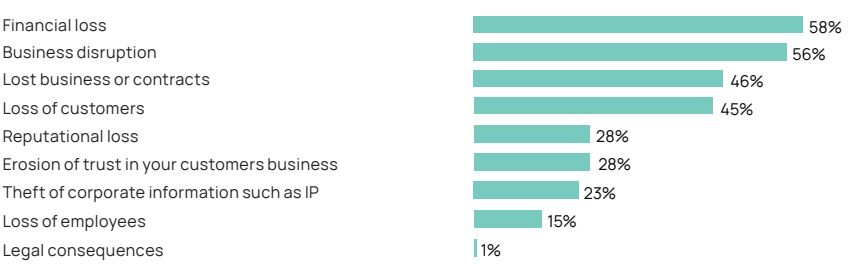
In line with the huge cyber-incidents witnessed this year, 55% of U.S. MSPs say they are targeted frequently by ransomware compared to only 34% of UK MSPs.

The cost of protecting customers

MSPs report that 82% of customers have seen an increase in attempted cyberattacks. And where attempted cyberattacks have increased, the average number prevented since the pandemic is now 14 per month, compared with 8 per month before it.

These attacks are having a devastating impact on both the MSP and end user communities, leading to a loss of customers, financial loss, and business disruption.

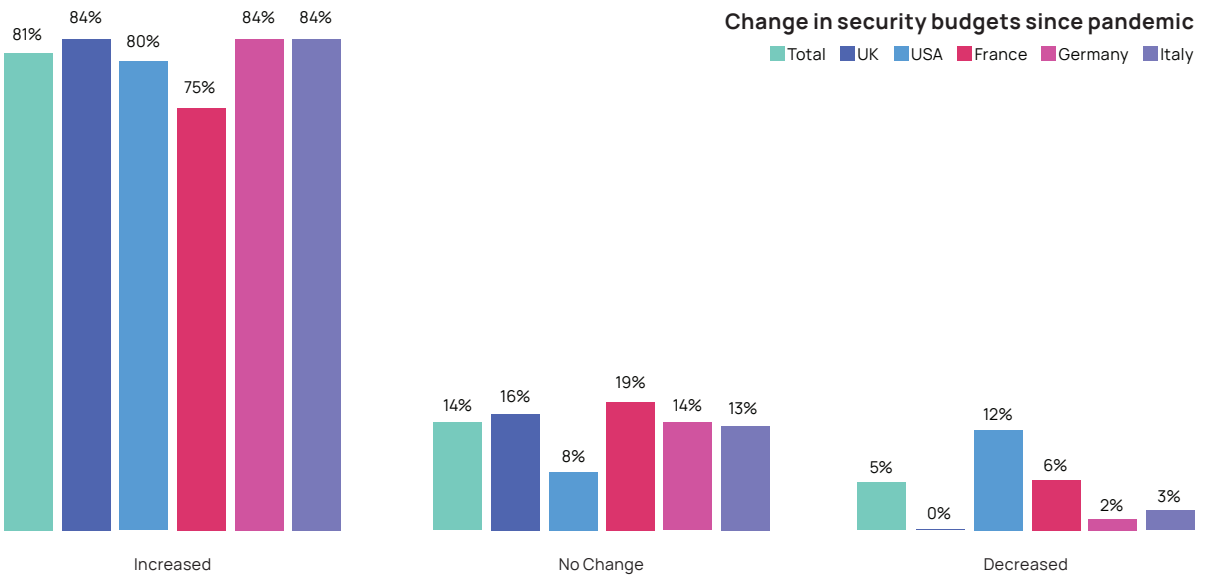
Impact cyberattack had on business



Our research shows that loss of customers was a particular issue in France and the U.S., while MSPs in Italy saw significant erosion of trust. The German and UK MSP communities encountered the greatest loss of employees due to an attack—at 26% for both regions.

MSPs are doing what they can in an untenable landscape

It's tough out there, but MSPs are trying to fight back. Four out of 5 of the MSPs we surveyed are increasing their security budget (though in France, it's only 3 in 4). The average increase is 5%; **France is slightly lower, and Germany slightly higher.** However, the question remains whether this is enough to combat the near doubling of direct attacks on MSPs.



81% of MSPs have increased their security budgets as a result of the pandemic compared to 70% of customers who have done the same. As MSP customers are spending a little more (7%), could MSPs afford to spend a little more to keep pace?

Where are MSPs spending their money?

The most common security tools receiving this extra investment include data security, cloud security, and infrastructure protection. Identity access is the least common investment. The toolsets MSPs are implementing include data encryption, antivirus, and multifactor authentication. There are also some interesting regional variations, with French MSPs investing heavily in VPNs, while the UK and Germany are putting money into email filtering solutions.

Implementing the basics is critical

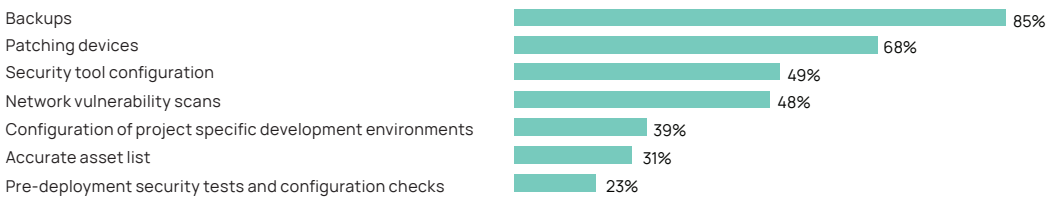
For MSPs to best protect their customers, there are several basics we have identified that need to be in place, but in some cases are being overlooked.

1. AUTOMATION IS CRUCIAL

With attacks increasing in both volume and sophistication, managing defenses manually is impossible. So, implementing greater levels of automation is essential to help keep customers' businesses secure. Here's what we're seeing in the market:

- **Automated backups** are the most common form of automation used by MSPs to keep their customers' businesses secure. It's used by 85% of all respondents and more than nine in ten of those in France and Italy.

Automation to help keep customer' businesses secure



- **Automated patching**—80% of MSPs are applying patches automatically.
- **Web filtering**—90% of MSPs are providing automated web filtering, though mostly URL based. Only around one in ten are using more secure DNS filtering.
- **Automated redeployment security tests and configuration checks** are currently used by less than a quarter of MSPs.

2. BACKUP IS CRITICAL—BUT WE NEED TO GET THE FREQUENCY RIGHT

Backup is crucial as the last line of defence in any attack—MSPs need to be able to recover their customers' data and systems no matter what. In general, backup is provided to most customers, but of major concern is the fact that only 40% of businesses are backing up workstations every 48 hours or less. The situation is better in France, where this figure stands at 60%. The news is better for servers as they are more frequently backed up, with 74% backed up every 48 hours or less.

Importantly, with more and more businesses moving their operation to the cloud, backup for Microsoft 365™ is offered by most MSPs, but there are distinct regional variations: All MSPs provide it in the US, but this drops to 87% in Germany.

> "Backup for Microsoft 365 is offered by most MSPs"

3. MULTIFACTOR AUTHENTICATION IS BEING IGNORED

While almost all MSPs offer two-factor authentication (2FA) to their customers, only 40% use it themselves. And despite it being offered, only a third of customers are currently using 2FA. However, MSPs report that they have plans to migrate 95% of customers to 2FA in the next five years, with most being done in the next two years.

Both MSPs and their customers appear to be deprioritizing identity management. While MSPs should give their customers what they want to some extent, there may need to be some tough conversations about prioritizing this key part of security hygiene.

> "Only a third of customers are currently using 2FA"

MIGRATION PLANS

2021 → 2026

33% → 95%

MSP cybersecurity is on government radars

Importantly for MSPs, against the backdrop of our survey, the global security landscape is changing. The agreement between the French and U.S. governments on cybersecurity is being replicated globally, with growing cooperation between technology vendors, IT services providers, and government bodies following several high-profile supply chain attacks in 2021.

Indeed, such was the threat of supply chain attacks involving MSPs in 2021, several governments have stepped in to attempt to mitigate the problem. For example, the UK government is moving forward with a proposed cybersecurity framework for MSPs. It argues there is a need to adopt "a more interventionist approach to improve resilience across supply chains, with regulation perceived to be 'very effective' by more respondents than any other suggested intervention."[2]

The interventions prioritized by the government will include legislative work to ensure that MSPs undertake "reasonable and proportionate cybersecurity measures."

This could require MSPs to adhere to a set of cybersecurity principles, such as having policies to protect devices and prevent unauthorized access. It would also require them to ensure data is protected at rest and in transit. Furthermore, it advocates for keeping secure and accessible backups of data, training staff, and pursuing a positive cybersecurity culture.

[2]https://www.gov.uk/government/publications/government-response-on-supply-chain-cyber-security

Conclusion:

Time for the unsung heroes of the pandemic to maximize the security opportunity

In many cases, MSPs have been responsible for keeping their customers' businesses running throughout the pandemic and ensuring they could manage the shift to remote working. As such, they have proven their worth many times over, becoming valued extensions to internal IT teams—particularly when in-house security pros were reassigned to help support employees that were working from home.[3]

However, MSPs cannot afford to let the trust they've accrued throughout the pandemic be eroded by a failure to protect their own systems. The reality is they are now being targeted by hackers in greater numbers than their customers, and in the same ways. And while many MSPs are responding by upping their security budgets and investing in new tools, the increases are small and may not be enough to combat the rise in attacks.

Focusing on the basics of cyber-hygiene is critical—especially with government regulation on the horizon. While many MSPs may address this with their customers, it is important they lead from the front, implementing the same technologies used by customers for their own businesses. The most critical areas our survey highlights are the use of MFA, alongside more regular backups, and a greater emphasis on automation.

The good news is that many MSP customers do not need to be convinced about the need to invest in security—they are already increasing their own security budgets and have priorities where they want to spend this. MSPs need to continue to be a safe pair of hands, and work with their customers to provide the security they both need, and demand.

[3](ISC)² Survey Finds Cybersecurity Professionals Being Repurposed During COVID-19 Pandemic (isc2.org)

Note: All statistics in this document are based on the findings of independent research commissioned by N-able.