SOPHOS

InfiniTech
Delivering Limitless Technology

The Impossible Puzzle of Cybersecurity

Results of an independent survey of 3,100 IT managers commissioned by Sophos

Sophos Whitepaper June 2019

Contents

The Impossible Puzzle of Cybersecurity

Results of an independent survey of 3,100 IT managers commissioned by Sophos

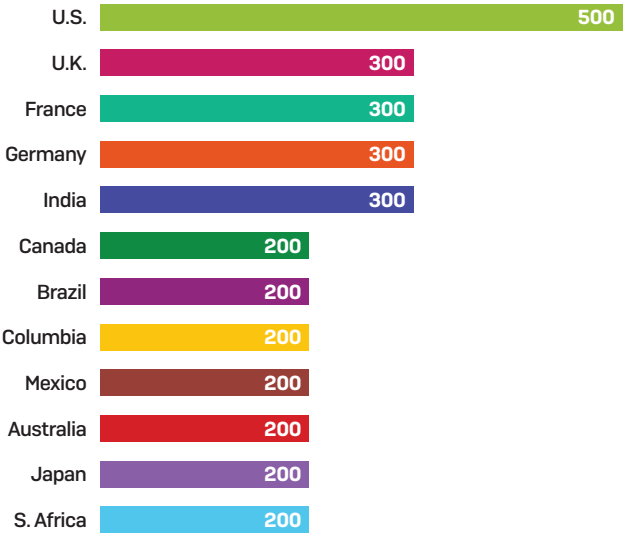
Cybersecurity just isn't getting any easier. While protection technologies continue to advance at a rapid pace, so do the cybercriminals trying to circumvent them. At the same time, the growing complexity of threats means that staying on top of them is an uphill task for stretched IT teams.

To understand these challenges, Sophos commissioned an independent study into the experiences of 3,100 IT managers across 12 countries. Conducted by research house Vanson Bourne, the survey reveals illuminating insights into levels and types of cyberattacks, and the difficulties managing cybersecurity.

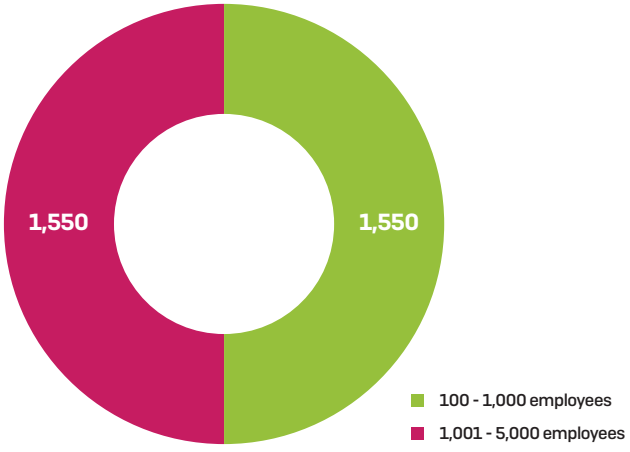
The Survey

U.K.-based research house Vanson Bourne interviewed 3,100 IT decision makers between December 2018 and January 2019. To provide a representative size split within each country, respondents were split equally between 100-1,000 user organizations and 1,001-5,000 user organizations.

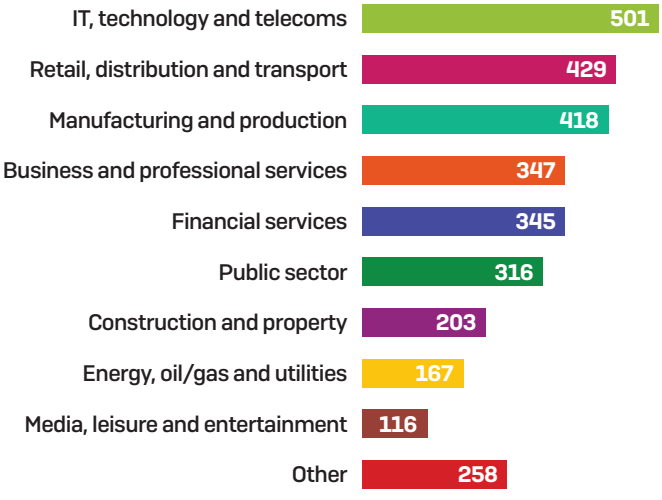
Number of respondents per country



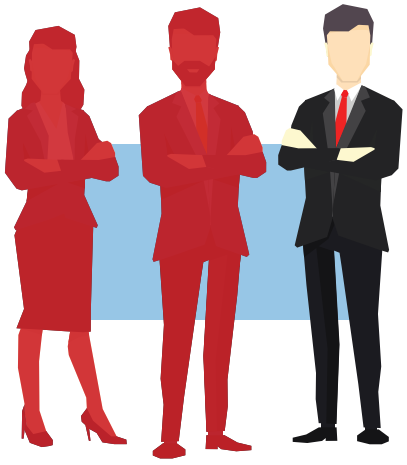
Split of respondents by organization size



Split of respondents by industry



Two out of three organizations fell victim to a cyberattack in 2018



All respondents were asked if they had fallen victim to a cyberattack in the last year, defined as a cyberattack that their organization was unable to prevent from entering their network and/or endpoints. 68% said yes. Of those organizations that had fallen victim, the average number of attacks was two, although 10% experienced four or more attacks.

Of particular concern, nine in 10 respondents (90.5%) said their organization was running up-to-date cybersecurity protection at the time of the attack – or in the case of organizations that suffered multiple attacks, at the time of the most significant one. Across the countries surveyed, respondents in France were most likely to have been running up-to-date protection (97.5%), while those in Colombia were least likely with only seven in 10 (70.9%) having up to date protection.

91% of organizations were running up to date protection at the time of the attack

This reveals that, despite good intentions and behaviors, threats are getting through. This may be through weaknesses in the cybersecurity, or because there are security holes that haven't been plugged or gaps in their protection – while an organization might have been running up-to-date endpoint protection, this doesn't mean all other devices were secure.

Cyberattacks lead to multiple areas of concern

The risk of cyberattacks leads to multiple concerns for IT managers, including:

Data loss The principal concern voiced by survey respondents with 31% rating it their #1 concern and over two-thirds (68%) considering it one of their top-three concerns.

Cost 21% of respondents considered the cost – both financial and time/effort – of dealing with the issue their primary concern.

Damage to the business Ranked a top-three concern by over half of IT managers (56%) and the #1 concern by 21%.

Interestingly, IT is clearly a team sport, with IT managers putting the wellbeing of the department ahead of their personal situation. 13% of respondents considered damage to the image of IT across the business their biggest concern from being hit by a cyberattack, nearly double the number (7%) that put personal job security at the top of the list.

Why organizations are still struggling to reduce cyber risk

As these results show, despite investments in security technologies, it's now the norm to be hit by a cyberattack. The survey revealed three main reasons why organizations are struggling to reduce cyber risk.

#1 Attacks come from multiple directions

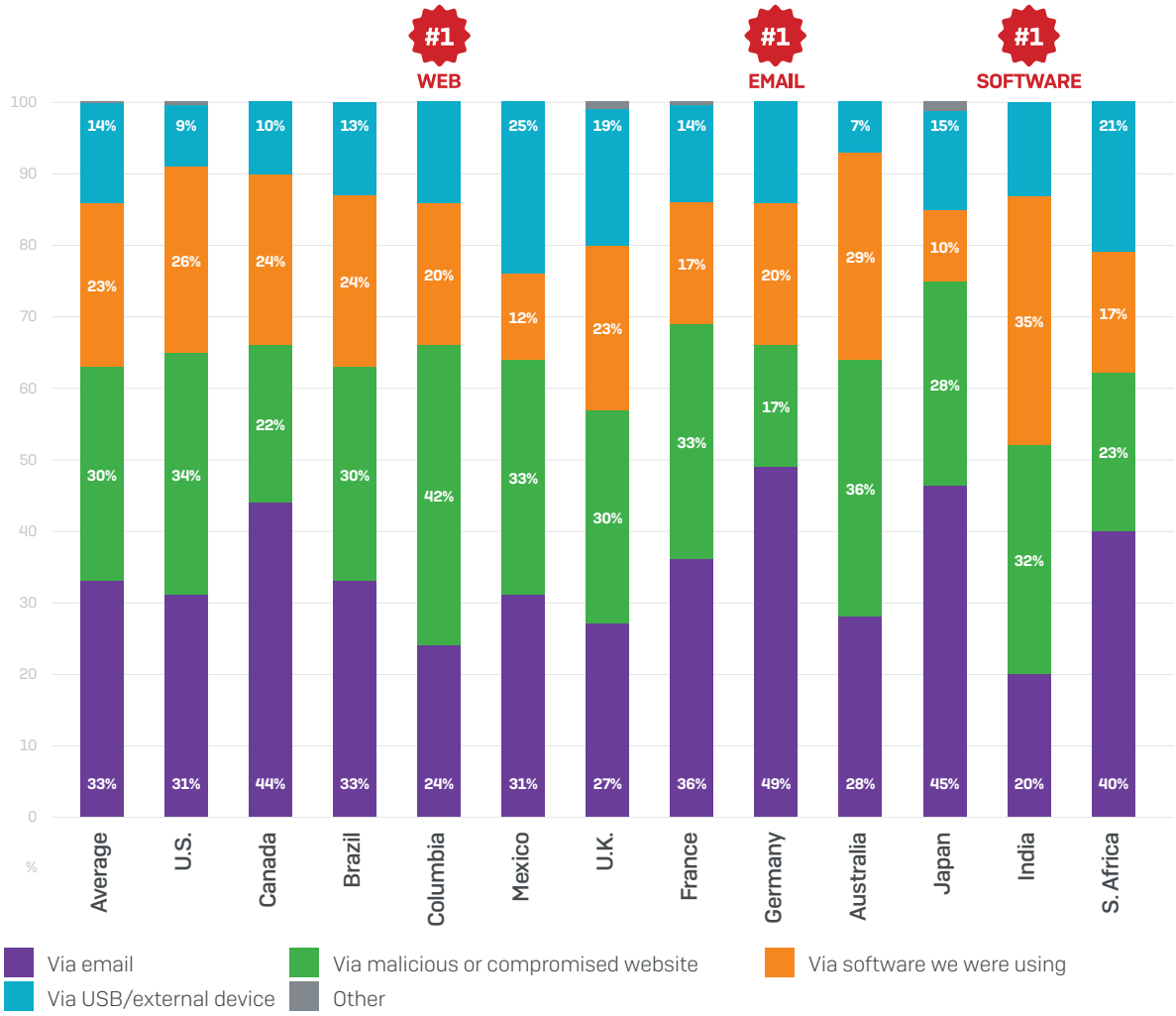
Respondents who had been victims of a cyberattack in the last year were asked how the most significant cyberattack got into their environment. The results revealed that, where respondents know how the attack got in, email is the most common attack vector, used in 33% of attacks. Given the prevalence of phishing (more on this later), this is no surprise. The web is also a major vector, used in three in 10 attacks. Together, email and web account for nearly two-thirds of attacks entering organizations.

IT managers can't just focus on email and web, however. 23% of attacks got in via a software vulnerability, and 14% via a USB stick or external device. Furthermore, 20% of IT managers didn't know how the most significant attack got in – if you don't know which security door has been left open it's hard to shut it.

How did the most significant cyberattack that your organization has been hit by in the last year, get into your organization's environment? (rounded to nearest whole number)
***Base:** Respondents who know how the attack got in (1,685)*

Diving into the data, it becomes clear that threat vectors vary greatly around the globe. The web is the most common attack vector in Colombia, while email is #1 in Germany and software vulnerabilities tops the list in India. USB sticks/external devices are the source of one in four attacks in Mexico.

This raises the interesting question of whether this variation is the result of bad actors using different attack vectors in different countries, or different security weaknesses across the geographies surveyed.



How did the most significant cyberattack that your organization has been hit by in the last year, get into your organization's environment? ***Base:*** *Respondents who know how the attack got in (1,685)*

IT teams have to manage a wide range of risks when it comes to cybersecurity. We asked respondents what they consider to be their top security risk. Given the attack vectors we've just seen, it's no surprise that phishing (#1) and software exploits (#2) feature high on the list.

However, in third position on the list is people, including internal staff, contractors, and visitors. We humans are ranked a top-three security concern by 44% of respondents, and clearly present IT teams with quite a different type of cybersecurity challenge.

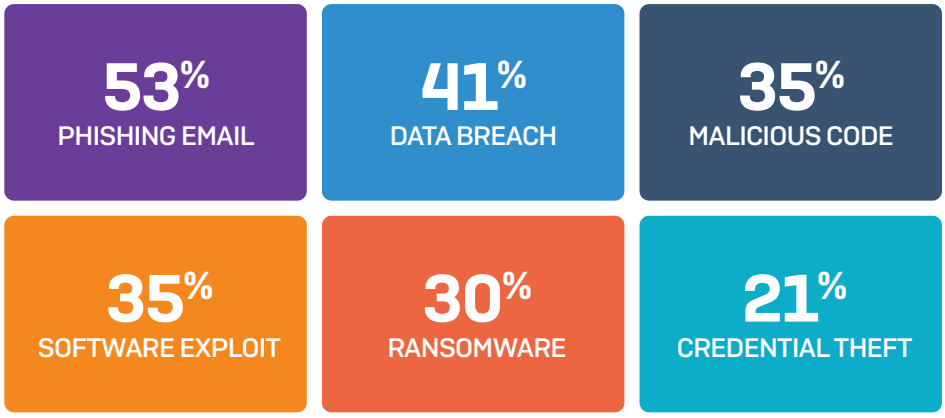
WiFi security also weighs heavily on the minds of IT managers with over one-third (36%) ranking it as a top-three concern, followed by unknown devices, which are a major concern for three in 10 respondents (31%).

What do you consider your organization's top security risks – combination of responses ranked first, second and third:

1. Phishing emails **50%**
2. Software exploits **45%**
3. People (staff, contractors, visitors) **44%**
4. Insecure wireless networking **36%**
5. Unknown devices **31%**

#2 Cyberattacks are multi-stage, coordinated, and blended

Respondents whose organizations had been victims of a cyberattack revealed that they had suffered a wide range of attacks over the last year.



What type of cyberattack(s) has your organization been hit with in the last year? ***Base:*** *respondents from organizations that have fallen victim to one or more cyberattack(s) in the last year (2109)*

These numbers clearly add up to more than 100%, indicating that multi-stage attacks are now the norm. For example, a phishing email could install malicious code that takes advantage of a software exploit to install ransomware. The high numbers involved also confirms the scale of the challenge facing IT teams.

Phishing: the most prevalent cyberattack

Of the 2,109 organizations hit by a cyberattack in 2018, over half (53%) were victims of phishing. Indeed, phishing was also the most prevalent attack in all countries surveyed with the exception of Colombia, where it was the second most common threat. Across the full 3,100 respondents, over one-third (36%) fell victim to phishing emails.

Software exploits: varied impact around the globe

Of the organizations hit by a cyberattack, over a third (35%) suffered from an exploit taking advantage of a vulnerability in software they were using. There are significant regional variations in propensity to be affected by exploits. In Mexico, over half of the organizations that fell victim to a cyberattack experienced a software exploit (51%). This is more than double the number affected in Brazil (22%), South Africa, and Japan (both 23%).

Ransomware: still alive and kicking

Despite rumours of the demise of ransomware, it is still very much alive and kicking. Three in 10 (30%) of the organizations hit by a cyberattack experienced ransomware. However this global average masks some significant regional variations:

- Half (49%) of Japanese respondents said they experienced ransomware, followed by the U.K. with 43%
- Just 5% of Mexican respondents experienced ransomware, and only 13% in Colombia

#3 Technology, talent, and time are in short supply

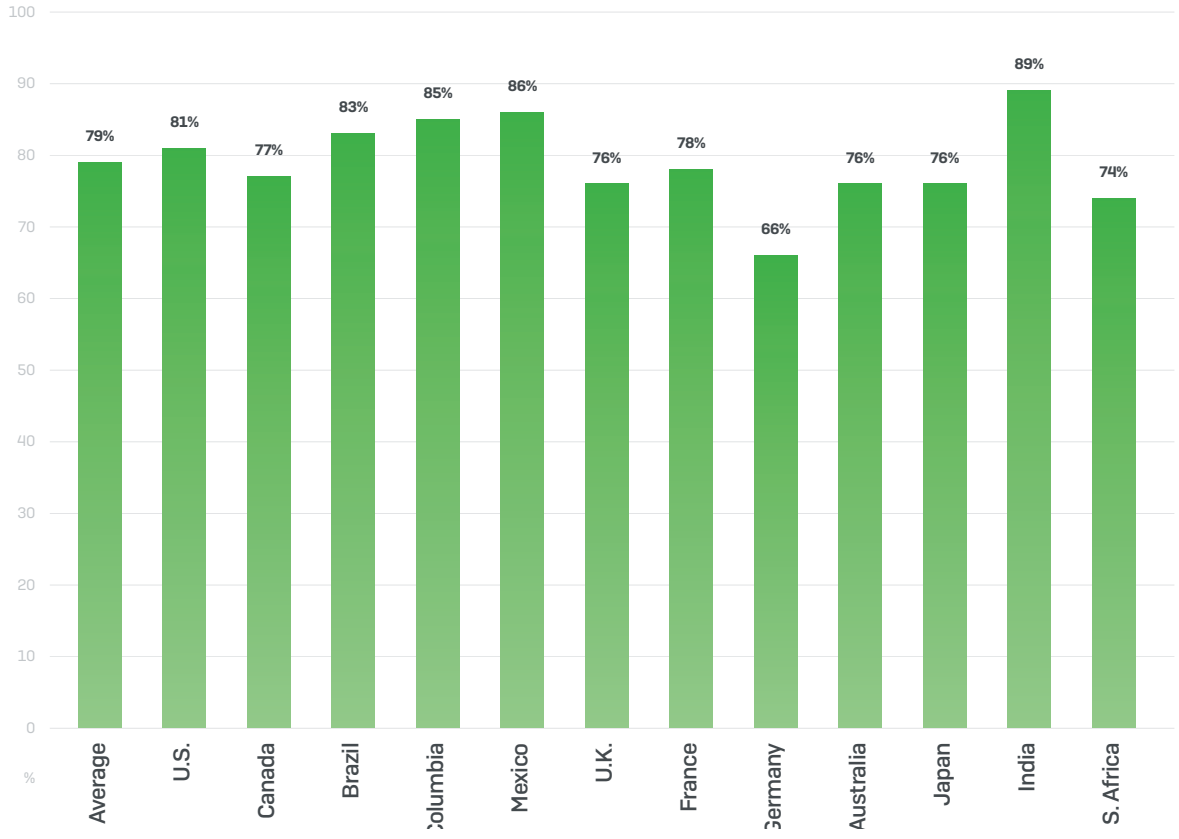
As we've seen, organizations face a wide range of attacks and need to secure multiple threat vectors. The survey revealed that, on average, IT teams spend 26% of their time managing cybersecurity. For the majority of respondents this is not the right ratio.

Indian organizations spend the most time (32%) and Japanese teams the least (19%). Organizations that had been hit by a cyberattack spend a little more time on IT security (28%) than those that hadn't experienced an attack (23%).

Given the variety and complexity of threats, it's not surprising that 86% of respondents say they need greater cybersecurity skills in their organization. Those organizations that had experienced an attack have greater need for cybersecurity expertise than those that hadn't (89% vs. 79%). This could be because they have more security issues that need fixing, or the result of heightened awareness of the complexity of today's attacks.

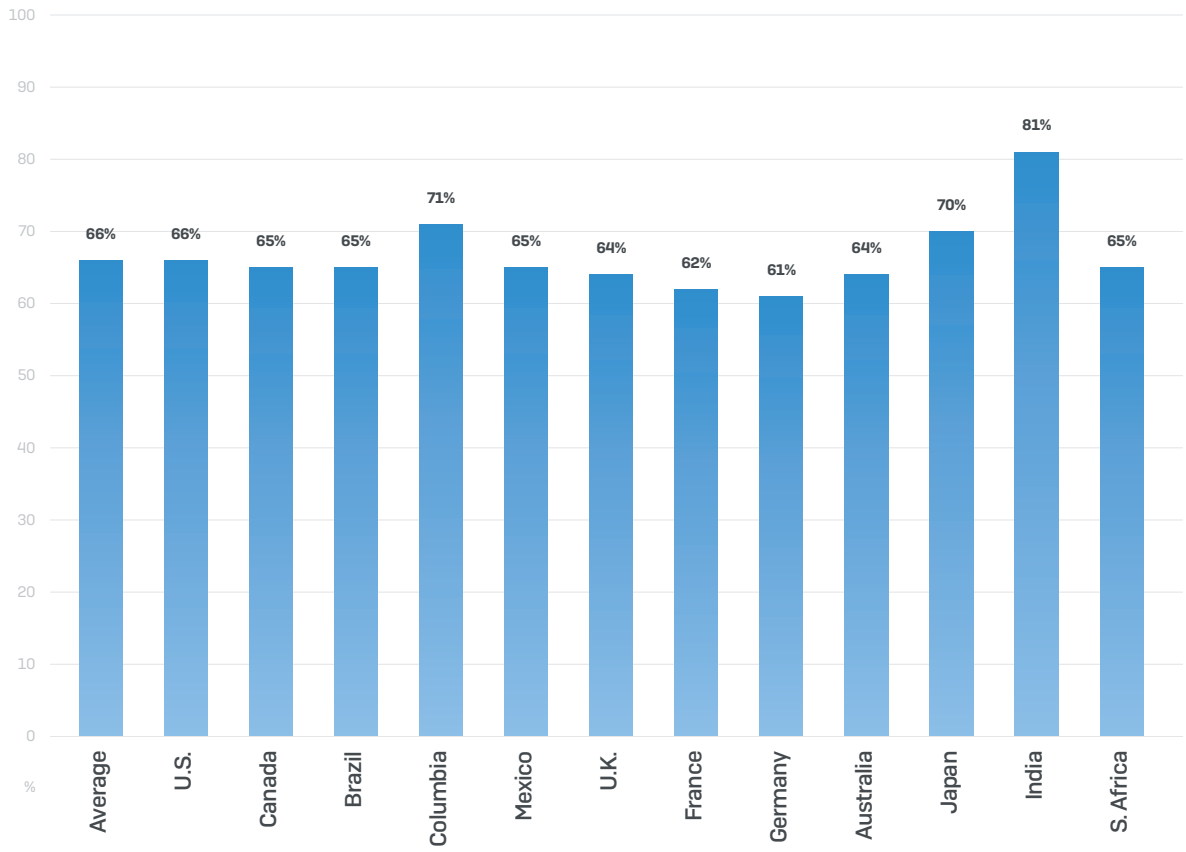
However, bringing in the expertise to fill these gaps is a major challenge. Eight in 10 organizations say they struggle to recruit in the right skills. When it comes to recruitment, India faces the greatest challenge (89%) and Germany the least – but still, two in three German IT managers say they struggle to bring in the right skills.

26% of IT team's time is spent on cyber-security



*Percentage of respondents that agree with the statement: Recruiting people with the cybersecurity skills we need is a challenge. **Base:** all respondents (3100)*

At the same time, cybersecurity budgets are not sufficient with two in three (66%) respondents saying that their budget for people and technology is too low. This rises slightly to 70% in those organizations that were hit by a cyberattack in 2018.



Percentage of respondents that agree that their cybersecurity budget (including people/ technology) is below what it needs to be. ***Base:*** *all respondents (3100)*

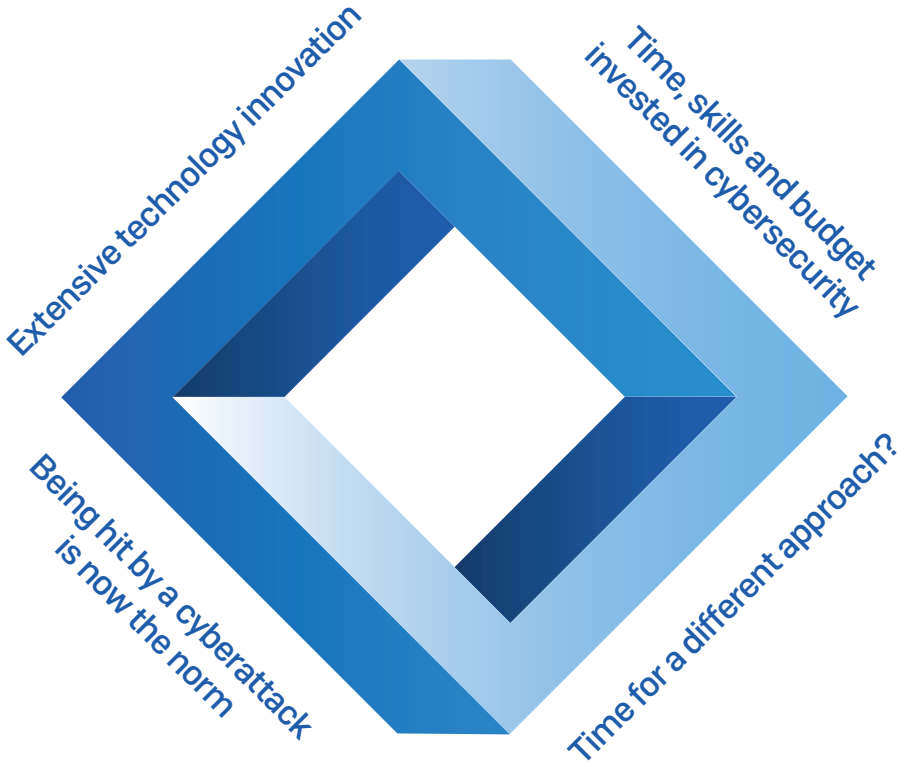
There are clear parallels between budget shortage and cybersecurity recruitment. Germany, the country with the least challenge when it comes to recruitment, also experiences the least budget shortages. Conversely India has the greatest budget challenge and also the greatest challenge with recruitment.

This reflects the limited supply of, and high demand for, cybersecurity skills, resulting in cybersecurity professionals able to command higher salaries and benefits packages.

The impossible challenge of cybersecurity

Technology companies have been developing cybersecurity products for decades, and organizations continue to spend time, effort, and money on cybersecurity. Yet, despite years of innovation and investment, the survey has revealed that cybersecurity remains an uphill challenge and organizations still don't have the resources they need.

Perhaps it's time for a different approach?



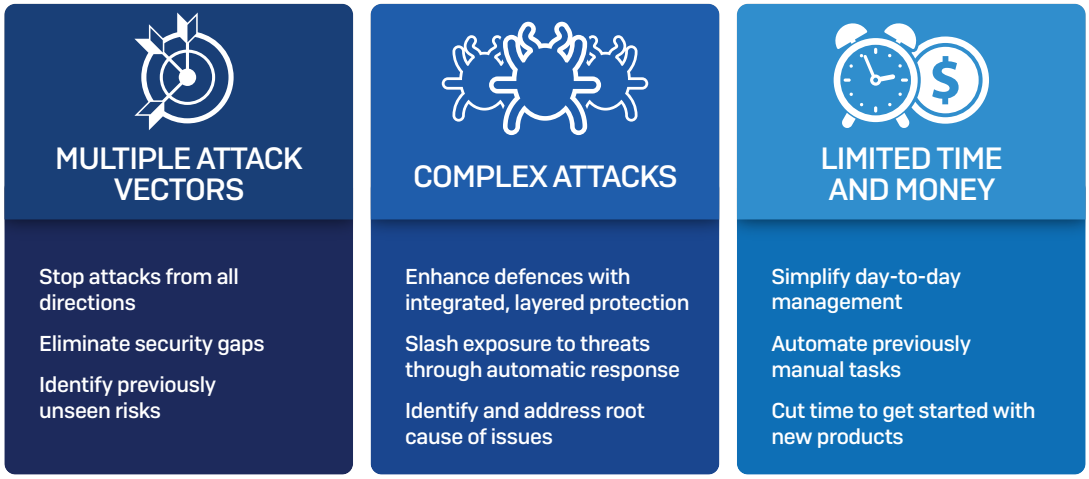
A different approach: cybersecurity as a system

As we've seen, cyberthreats work as a system using multiple interconnected techniques and technologies in their attacks. At the same time, our IT infrastructure is also a system – a complex, inter-connected network of PCs, Macs, servers, printers, mobile devices, apps, cloud workloads, switches, printers, firewalls, wireless systems… and all the software that runs on them. With IT infrastructure and cyber threats both working as a system, it makes sense that cybersecurity should also work as a system rather than isolated point products.

Synchronized Security is Sophos' award-winning cybersecurity system. Endpoint, network, mobile, Wi-Fi, email, and encryption products, all sharing information in real time and responding automatically to incidents. And with everything controlled through a single, web-based console, management is a breeze.

Synchronized Security: solving the impossible puzzle

Synchronized Security enables organizations to address the complex challenges revealed by the survey.



Multiple attack vectors:

- The complete portfolio of protection enables you to stop threats from all vectors of attack: email, web, software vulnerability, USB devices.
- The products are engineered to work together, eliminating security gaps as well as avoiding compatibility issues.
- Unprecedented insights let you identify previously unseen risks, such as malicious apps in the network traffic.

Complex, coordinated, and multi-stage attacks:

- Integrated, layered protection maximizes your defenses against advanced threats by blocking them at multiple stages and using multiple technologies.
- Automated incident response slashes your exposure to threats by stopping and isolating attacks in seconds.
- Cross-estate insights enable you to identify and address the root cause of any issues.

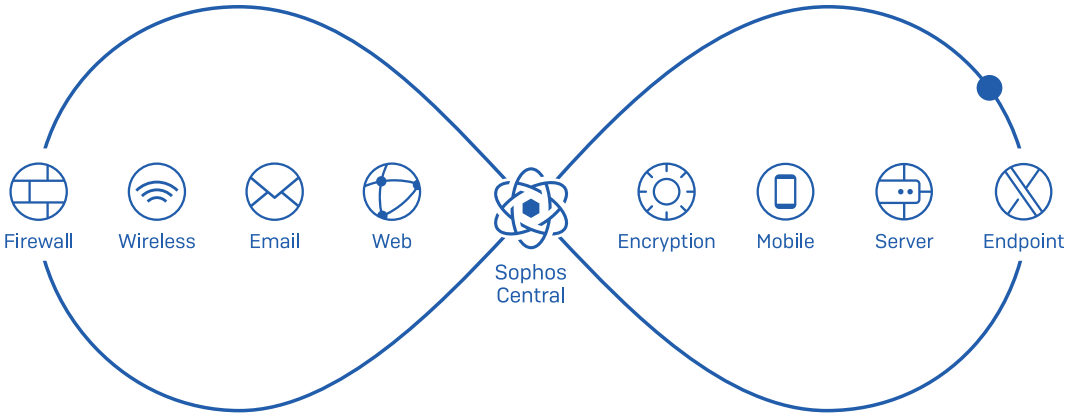
Time, talent, and technology in short supply:

- Managing everything through a single, web-based console significantly reduces day-to-day overheads while freeing up team members.
- Automated incident response also relieves the admin burden on IT by removing the need to manually identify and remediate infected machines
- The consistent, familiar interface across all products makes it quicker and easier to get started with new products.

Conclusion

Despite heavy and ongoing investment in cybersecurity technology, the job for IT teams across the globe isn't getting any easier. Rather than continuing further with the same approach to cybersecurity, it's time to move to cybersecurity as a system. By enabling security products to share information and work together in real time you can stay ahead of the threats while also freeing up valuable IT resources.

Sophos Synchronized Security is the award-winning cybersecurity system trusted by thousands of organizations across the globe. To learn more and see it in action visit www.sophos.com/synchronized.



To learn more and give it a try visit www.sophos.com/synchronized

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

19-06-21 WP-NA (RP)

InfiniTech Delivering Limitless Technology

SOPHOS