The Positive Way

WAVESTONE

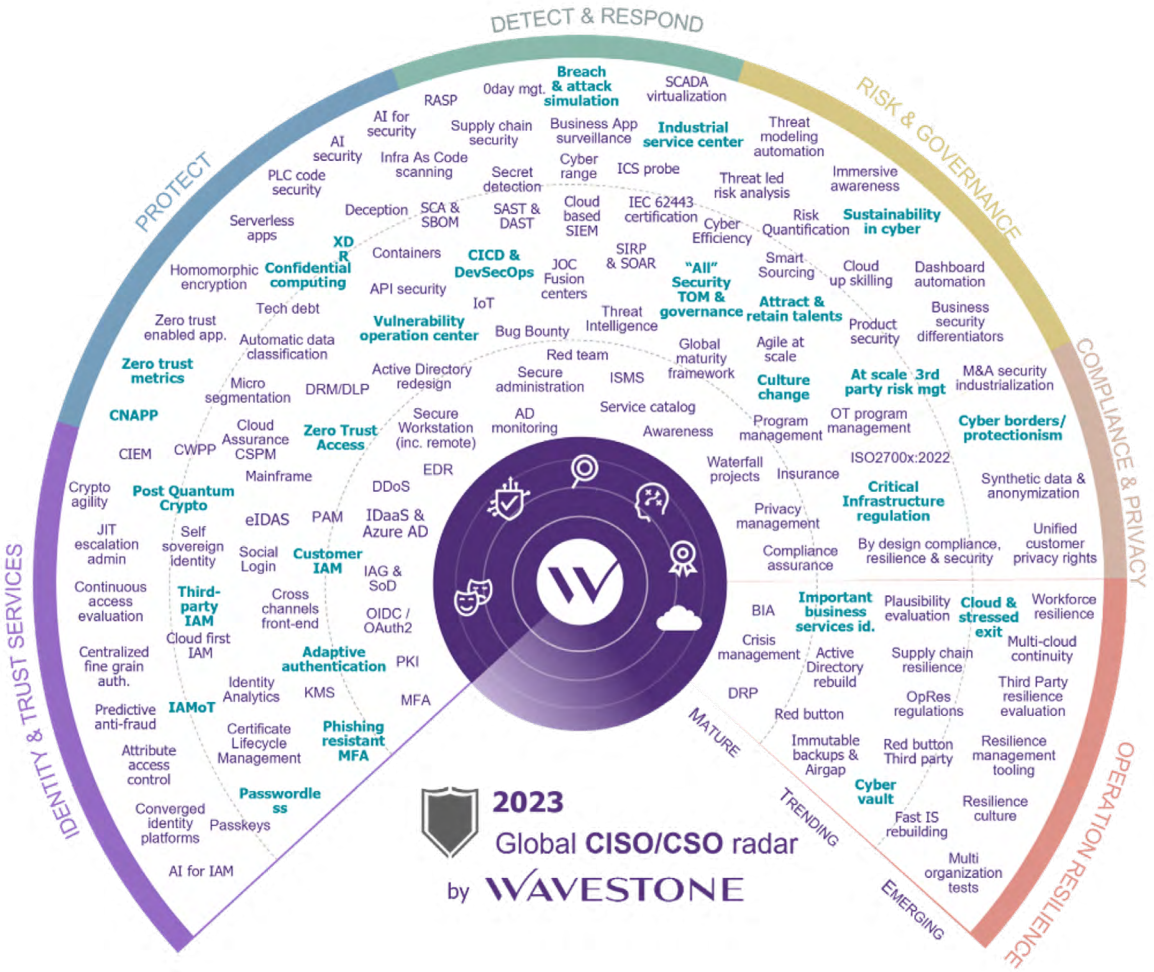
Special Report

CISO RADAR:
TOP SECURITY PRIORITIES FOR 2023

2023 WILL BE A YEAR OF TRANSITION TO A BETTER MODEL FOR CYBERSECURITY AND RESILIENCE

News of the last few months has confirmed the importance of cybersecurity for large organizations. **Under the influence of new geopolitical dynamics and acceleration of digital transformation activities, international companies have become aware of necessary investments.** Changes that have been initiated will accelerate in the coming months because of pressure from regulators and the need to align with new organizational practices and technological innovations.

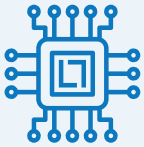
Each year, Wavestone's **CISO Radar** report analyzes the highlights of the past months and the key challenges for the months to come. It summarizes the key issues observed by our clients – very large public and private organizations on an international scale.



CRITICAL CYBER TRENDS IN 2023

Regulatory requirements will compel a number of players, especially financial organizations, to meet more rigorous security standards. This is true whether your company's mission is financial services or to the financial group within your organization supporting a different mission.

Organizational challenges: cyber teams are facing new difficulties recruiting and retaining specialized skills; this broadens the CISOs' scope to include managerial and mentoring roles.



Technology development highlights Zero Trust, Cloud security, industrial security, and vulnerability management.

Geopolitical landscape calls for organizations to re-assess their cyber strategy (physical relocation of activities, security of third-parties) for broader and deeper dependability, resilience, and effectiveness.

LOOKING BACK AT 2022, A YEAR OF CHALLENGES AND SUCCESSES FOR CYBERSECURITY

An increasingly structured response to ransomware threats

For several years now, **cyber villains have favored ransomware attacks. Hospitals and local authorities are amongst the most publicized victims.** However, regardless of industry sector, hackers prefer **"double extortion"** as well as exploitation of third-party vulnerabilities. The ANSSI's Panorama of the IT threat, published in March 2022, also reveals that state-sponsored threats are still growing, particularly in terms of espionage.

To combat these threats, large organizations are continuously investing in cybersecurity, and these efforts are indeed paying off: **the number of disrupted attacks continues to grow!** Most organizations now have integrated prepared incident response teams and effective protection tools. And this evolution will continue to be part of a new, better model for enterprises to address cybersecurity and resilience with greater efficiency.

Internally, however, there is still strong pressure for organizations to obtain the necessary cyber resources. Human resources are still a challenge for the progress of such projects. Despite their growth, budgets allocated to cybersecurity remain relatively low in many sectors, especially public ones. The good news is that those who have completed their remediation programs are seeing greater stability in their budgets, freeing them up to address the increasing pressure to demonstrate effectiveness.

Double extortion ransomware is a type of cyberattack in which threat actors exfiltrate a victim's sensitive data in addition to encrypting it, giving the criminal additional leverage to collect ransom payments. A traditional ransomware attack will only encrypt a victim's data. The added threat of exfiltration makes this attack more dangerous for organizations in all industries.

Focus on the Russian-Ukrainian conflict

In Europe, the Russian-Ukrainian conflict has raised many concerns about cybersecurity. The digital resources deployed are substantial, and the attacks are destructive but targeted. However, at the time of writing this article, the feared cyber outbursts have not yet become reality. **A bigger surprise came from acts of cyber resistance, through hacktivists taking sides with one or another of the two camps.**

In Belarus, for example, pro-Ukrainian activists paralyzed the national railway system to slow the Russian breakthrough. This mobilization was even orchestrated by the Ukrainian state with the launch of an "IT Army". The Russian camp did not remain passive, launching waves of attacks on structures and organizations supporting Ukraine.

Even if the offensive attacks were to follow, the cyber impacts currently remain manageable for the moment by large organizations. This is explained in part by proactive initiatives, in particular by reinforcing surveillance levels. Risk management has also covered these preventative actions: exploration of dependencies, reflection on network isolation capabilities, implementation of additional security measures, particularly against denial-of-service attacks, etc.

Cyber regulation: busy season

On the government side, regulatory work continues to grow and the legal framework is being strengthened.

01 In the United States

Government regulators in the US are significantly increasing initiatives. In the financial sector, for example, the new requirements of the NYSDFS (New York State Department of Financial Services) provides needed support to companies in terms of recruitment and financial resources.

02 In Europe

It has been a particularly active year in Europe!

/ The Cyber Resilience Act establishes common protection rules for connected products.

/ The European Commission adopted the new version of the Network and Information Security (NIS) directive: NIS 2. The text harmonizes and extends the scope of the directive dedicated to critical infrastructures.

/ The Digital Operational Resilience Act (DORA) came into force in 2022 and will become the referenced regulation in terms of operational resilience, particularly in the financial sector.

/ The European Cybersecurity Certification Scheme for Cloud Services (EUCS), spearheaded by the European Union's Cybersecurity Agency (ENISA), is paving the way for new standards to label the most secure cloud solutions; however, discussions remain complex and there is more to do here.

03 In Asia

Regulations are also significantly increasing in Asia, including China, particularly in the area of privacy protection, with very different approaches and objectives depending on the country.

The emergence of new regulations affects cybersecurity players in a paradoxical way. On one hand, this regulatory attention is a lever to release funds and deploy large security programs. On the other hand, the prescribed actions are extremely mobilizing of cyber resources and take teams away from their focus on other high value-added cyber actions. Some measures required by newer regulations can become disconnected from current operational priorities; i.e., they can generate deep modifications of the information systems that make daily management more complex. In the years to come, the construction of a functional and legal framework will require a continuous and constructive dialogue with regulators.

CISOS HAVE A ROLE TO PLAY IN STRUCTURING THE INDUSTRY!

In 2023 (and beyond), profound regulatory, organizational, technological and environmental transformations will permeate the cybersecurity field. The industry must re-think and re-design its strategy adaptively in light of these changes.

Retaining cyber experts: the winning HR choice

Cyber strategies can no longer perform without a human factors perspective to effectively maintain their security level. **The first question CISOs should ask themselves is "make or buy?"** In other words, should the organization internalize the needed cyber skills, or outsource resilience or response activities to a third-party?

Historically, the decision has been to turn to outside providers for such needs designated as temporary; while security was viewed as a necessary evil or cost center. Today, keeping cybersecurity in-house is becoming a growing business concern because of the increase in resilience issues, new ever-evolving levels of product security, requirements for additional financing of cyber solutions, and of course the omnipresent interests of customers and partners. Going forward, it seems essential to adopt a Smart Sourcing approach that flexibly encompasses all these needs.

In a tight market like the one we are experiencing, an effective HR strategy is based on two pillars: talent recruitment and talent retention. The former sometimes requires creativity! For example, you might decide to recruit non-specialist profiles who you believe can be trained. Or perhaps you can create new avenues of internal mobility, allowing people to enhance their skills without leaving the company.

Once the cyber team has been built, it becomes crucial to retain key employees.

Salaries are certainly a lever for attractiveness. But beware, they are also a reason for departure. The cybersecurity sector reveals growing salary disparities between sectors and, on a larger scale, between countries.

Knowing the key profiles, competencies and interests of your people allows you to arbitrate between skills expertise and management, while giving clear objectives and a career path adapted to each person. **This is a real resource management transformation for cyber teams!**

Continuous training for each type of cyber resource profile is also a retention tool. It also benefits the organization's ongoing security posture. Be sure your career path strategies include both initial training for non-cyber profiles and expertise paths for advanced profiles.

Sector-specific issues: Focus on cyber in Industrial and Finance

The security of industrial production sites is making strong progress, although there is still a long way to go in terms of the backlog and the lifespan of installations. Meanwhile, manufacturers are increasingly digitizing their production and selling associated digital services, **product security remains in its infancy. It is an element of differentiation between manufacturers today; but will be a prerequisite for all manufacturers tomorrow.**

This is the time to evaluate your manufacturing, sales, and after-sales cycles, and to take action on cybersecurity proactively. These developments also require the creation of separate communications and process channels that are integrated with the historical management of Information Systems.

The financial sector, for its part, is restructuring the cyber sector and related sectors (i.e., IT risk, fraud, security of goods and people, etc.) in response to the increased demands of regulators. In particular, resilience is becoming the focus of transformation programs, with its share of new issues: identification and mapping of critical services or ability to quickly exit a platform or a third-party service (a "stressed exit"). This phenomenon is growing in the United Kingdom, but is only just emerging in the United States and France.

Focus on CISOs in the Financial sector: from CISO to CSO (Chief Security Officer), an ongoing transformation

Organizational and sectoral transformations are broadening the responsibility scope of CISOs to include subjects that were not previously within their purview, such as anti-fraud, operational resilience and physical security.

The CISO profession is undergoing a profound change that makes it much more than a technical and legal expertise function. In response to the professionalization of cybersecurity, CISOs are now expected to adopt a managerial posture (budget management, team management, etc.). To support this change, companies and administrations are turning to specific training, internal coaching, or even the recruitment of a non-expert profile with knowledge of the organization to support the CISO.

This trend is expected to spread to other sectors in 2023 and over the next few years.

Opinion from Cybersecurity Expert Oliver Newbury, Barclays CISO

Oliver Newbury, Global Chief Information Security Officer of Barclays

shares his opinion on the 2023 landscape, with a specific view on what will be key in the Financial Services sector. He provides advice on what CISOs should focus in 2023 in order to keep the business secure.

In 2023, companies must continue to enhance their digital capabilities and also exploit cloud platforms in order to remain competitive.

In response, CISOs must tailor their security approach to enable new technologies, whilst ensuring the organization is safe against a highly volatile geopolitical backdrop.

In the Financial Services sector, customers and clients' expectations of high quality digital experiences is continually increasing. *CISOs must evolve their approach to better enable technology teams to develop faster through tech DevOps practices and apply the right techniques to enable data to be analysed securely.*

Larger, more traditional organisations carry a high risk. They manage a large profile yet are challenged with keeping up with the pace of change and ultimately transforming the way technology operates in order to meet customers' expectations. It's the CISO's job to make sure this is done securely.

CISOs must enable the business to adopt new technology and keep it secure. And this will be key in the year ahead.

Oliver Newbury, Global Chief Information Security Officer, Barclays

MAJOR TECHNOLOGICAL CHALLENGES FOR CYBERSECURITY IN 2023

The continued road to Zero Trust

In addition to organizational issues, the market is adapting around new security solutions to support digital transformation. This transformation is driven by a generalized “Move to Cloud” in all sectors, a reconciliation between operational technology and IT within the industrial world, and expanding the access of information systems to numerous partners, acquisitions or customers.

This movement is leading to tactical responses in cybersecurity, with the emergence of tools to better control ongoing projects (see box below on the Cloud in particular). In the near- to medium-term, the atomization of the information systems continue and will require a rethinking of the security model – towards Zero Trust logic.

A simple philosophy, Zero Trust, has been gaining momentum for a long time. The principles are being translated into concrete measures, and new solutions are appearing; as an example, the publication of the first frameworks such as that by the Department of Defense (DoD) in the United States.

The feedback from this experience has been very positive, particularly in terms of remote access and micro-segmentation. For anticipated challenges to come, we think of identity and access management, for employees, partners, customers, and, increasingly, also for machines and data, with the established IDPs (Identity Providers). However, the road to a complete migration of information systems seems long and may not be of interest for legacy systems, which will need to be protected in other ways.

Application and CI/CD platform security: the next frontier

CI/CD applications and platforms are the next preferred areas of threats for cyber attackers. Therefore, putting them under control soon is essential. Security and DevSecOps approaches must be at the heart of development teams’ activities in order to integrate the necessary protections as early in their lifecycle as possible (with the widely adopted “shift left” movement, to position security as close as possible to developers and testers to make them accountable).

The agile mode has significantly integrated security teams into the application lifecycle starting with design. Hence it is necessary to increase the number of technological safeguards throughout the Software Development Life Cycle (SDLC). The issues concerned range from training to source code auditing, management of secrets on development platforms, securing containers, and the implementation of software bills of material (SBOM).

Better manage third-party risks

Many attackers take advantage of security holes in third-party systems to breach an organization. The first step in limiting this type of intrusion is to identify the partners and service providers that should be given priority in security remediation. **The usual criterion of volume of revenue generated is not always the right one to evaluate the managed risk of data leakage or service interruption.** Smaller third-party providers may hold more critical information or provide a link in a critical service.

For the most critical third-parties, it is necessary to consider reinforcing contractual commitments and reporting in terms of security. **To go further, take into account this risk as it lives within your processes,** whether it is the management of incidents affecting third-parties, the ability to integrate them into access management systems, or even if viewed as their own level of cyber resilience.

Third-party management platforms are one way to centralize these concerns and activities. Platforms that will be as useful in prevention for resilience analyses, or the definition and monitoring of requirements implementation, as in reaction when an incident does occur.

Tactical solutions for cloud security

2022 has seen the democratization of solutions allowing better control and management of the security of cloud platforms: for instance, the CNAPP (Cloud-Native Application Protection Platform) is a global management platform for the entire cloud ecosystem. This tool can be coupled with the CWPP (Cloud Workload Protection Platform), a solution designed to secure platform payloads.

For access rights, CIEM (Cloud Infrastructure Entitlements Management) is a tool for managing the complexity of services and their related access rights. The presence of these tools is growing amongst our clients; and their implementation is often quite easy, but their daily use remains a subject to be dealt with because they require higher levels of cloud technologies skills.

Recent progress to build upon today

1

Passwordless

Passwordless, to finally free the user from the antiquated password, is becoming popular with major technology players and its democratization is increasingly paving the way for use in large organizations. Even if it can't be used everywhere and for every action, this technological evolution allows organizations to send out a positive and less constraining image of cybersecurity.

2

Vulnerability management

Vulnerability management remains a complex and necessary topic where the market is still struggling. Major incidents like LoG4J have shown the limits of current vulnerability practices. New initiatives are emerging with the creation of Vulnerability Operation Centers, centralizing expertise and giving substance to a subject that is usually spread too thin across the organization.

On the other hand, new management platforms are being deployed, allowing for more refined prioritization according to each threat and applying more industrial management. An emerging movement is underway with the transfer of asset management capabilities, which was historically on the production side, to now be on the cybersecurity side. It will be interesting to see if this trend continues and solidifies.

3

The three anti-ransomware pillars: MFA, EDR and AD monitoring

As most of our clients have learned from cyber incidents, user workstations and devices are still the primary entry point, and the Active Directory is a primary target of ransomware groups.

Investing in the security of these elements, by deploying multi-factor authentication (MFA), Endpoint Detection and Response (EDR), and by hardening and monitoring the Active Directory (AD), are essential and effective points. Even if nothing is perfect, 2022 has seen many progressive anti-ransomware deployments and the feedback from our customers demonstrate their usefulness and effectiveness, resulting in a decrease in successful ransomware attacks on large accounts.

In general, the market for cybersecurity providers remains extremely dynamic. But 2022 has confirmed a fundamental trend towards the transformation of the role of the major cloud players into cybersecurity solution providers.

This is the case of Google, for example, which clearly displays this strategy with the recent acquisition of Mandiant. With this move, Google is creating an entity specialized in cybersecurity, affirming its desire to compete with Microsoft in cyber activities. The key question for 2023 and years to come will be the level of independence that we wish to keep (or will be able to finance) between IT production activities and detection/protection tools if a single player attempts to manage them all.

WHAT ABOUT TOMORROW? RETHINKING SECURITY IN A RAPIDLY CHANGING GLOBAL CONTEXT

The unstable geopolitical context shows us that it is important to keep in mind the risk of fragmentation of the Internet. The recent Russian-Ukrainian conflict has made the European continent aware of the proximity of certain threats and the potential impacts on information systems. In a return to a form of protectionism, regulations are accumulating in the four corners of the globe, forcing companies to adapt their information storage and systems, and their use of local technologies.

This trend towards de-globalization will have to be reflected in the definition of cyber strategies for large, internationally-situated groups. They must take these constraints into account when analyzing risks, especially when using local platforms, as well as when looking for solutions to guarantee the security of global exchanges without compromising compliance with local requirements.

Although this movement is becoming more prevalent, it does not affect all companies in the same way and requires a multi-dimensional response. The organization must be prepared to deploy a rapid response to be activated in the event of a conflict that has an immediate impact on its structure and systems.

Some of these measures have already been developed and tested to isolate one's self from partners or subsidiaries undergoing cyber attacks. But in the near future, CISOs will also have to think about guaranteeing the global security of the organization by relying on disparate systems in different geographical areas and, more broadly, to think about the resilience of their globalized organization in the face of geopolitical developments and their cascading impacts on information systems.

Finally, at a time of global environmental transition, it is becoming crucial to adapt cyber systems and tools to the requirements of sustainability and reduced environmental impact. Several green cyber initiatives are beginning to emerge, indicating the desire of organizations to think proactively about responsible cybersecurity and optimizing the use of their resources.

The emergence of these new risk profiles requires organizations to undertake a deep reflection on their new 2023-2026 strategic cycle by integrating the new business challenges of their sector.

METHODOLOGY

Every year since 2011, Wavestone's cybersecurity experts have been deciphering global trends in the **CISO Radar.** More than 40 experts from all over the world share their vision based on real cases observed at their clients' sites.

The CISO Radar presents a selection of items that cybersecurity professionals have to deal with in their daily operations. It is organized into quadrants that delineate key themes: Identity & Trust Services; Protect, Detect & Respond; Risk & Governance; Compliance & Privacy; and Operational Resilience. Each of these themes is divided into three levels of maturity: "Mature," "Trending" and "Emerging."

1. "Mature" topics can and should be mastered by any CISO.
2. Topics categorized as "Trending" are beginning to be addressed operationally; initial feedback is available.
3. "Emerging" subjects are still not well known or as yet have no obvious solutions. Identifying them allows you to anticipate future developments and prepare for their arrival in your organization.

About Wavestone

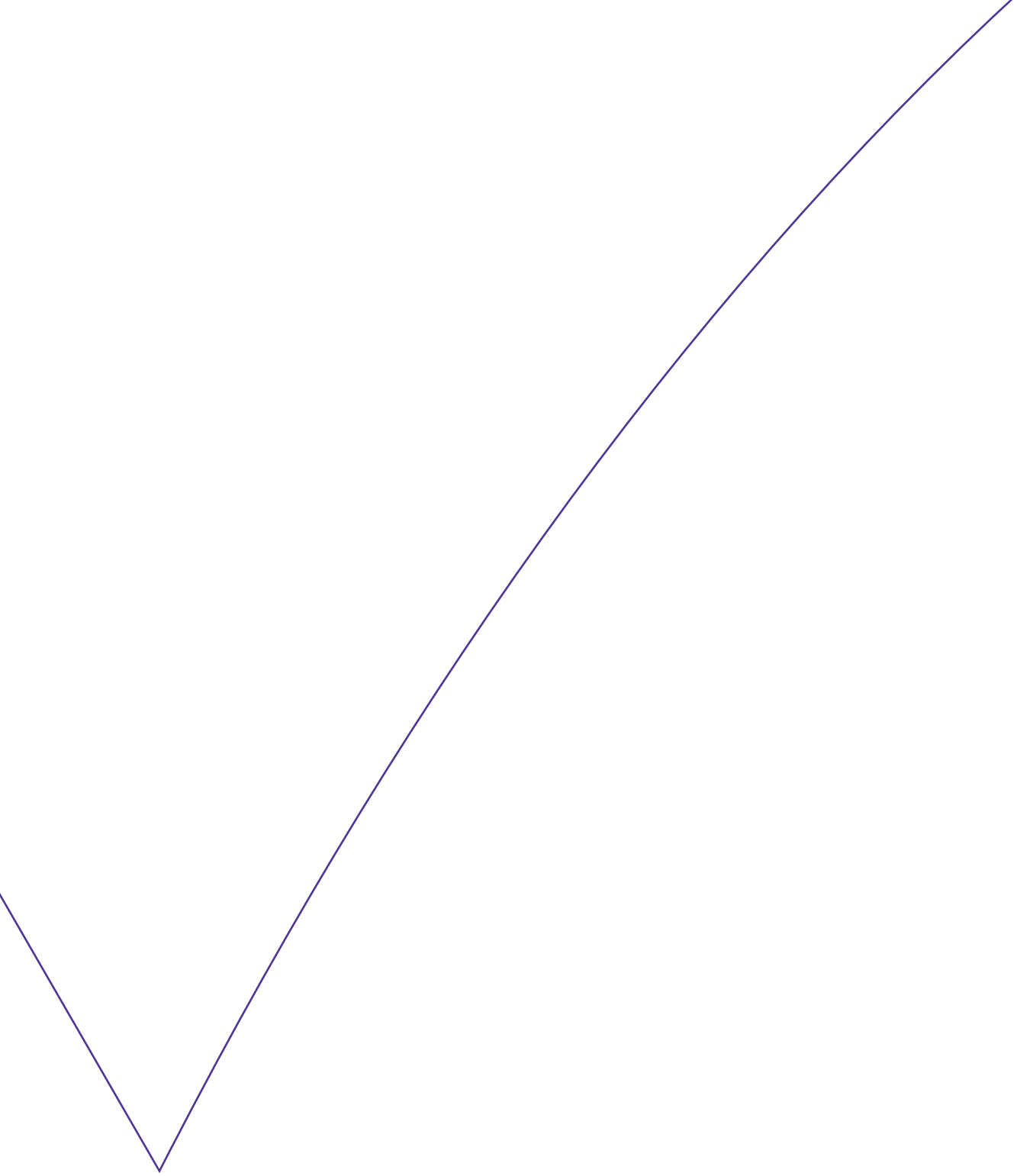
Wavestone is a global leader in the field of cybersecurity. Our 700 cybersecurity consultants combine functional, sectoral, and technical expertise, and cover more than 1,000 engagements annually. Wavestone experts provide thought leadership to the industry and present at conferences around the world. And every year, we publish our CISO Radar to help CISOs better understand the issues in front of them.

To learn more about Wavestone's cybersecurity capabilities and how we could support your organization, please reach out to **florian.pouchet@wavestone.com**

You can also visit **Wavestone Cybersecurity.**

WORLD'S BEST MANAGEMENT CONSULTING FIRMS | Forbes 2022 POWERED BY STATISTA

Forbes Names Wavestone among World's Best Consulting Firms 2022



The Positive Way

WAVESTONE

www.wavestone.com

In a world where knowing how to drive transformation is the key to success, Wavestone's mission is to guide large companies and organizations in their most critical transformation projects, with the ambition of a positive outcome for all stakeholders. That's what we call "**The Positive Way**".

Wavestone brings together 4,000 employees across 9 countries. It is a leading independent player in the global consulting market.

2023 © WAVESTONE