CISO AT THE HEART OF THE IS REVOLUTION

2019 TRENDS AND THE CISO RADAR

What are the key points to draw from today’s welter of cyber issues?

Cybersecurity is in constant flux: experiencing ever-evolving threats and regulations, but also a profound renewal of the way information systems (ISs) function. Faced with this raft of changes, distinguishing the substantive trends, and setting an appropriate cybersecurity strategy, can be challenging. With this in mind, experts from Wavestone’s cybersecurity teams meet regularly to discuss market trends, and identify core issues, new topics, and emerging technologies to be explored. This year, these reflections have resulted in an in-depth analysis of the major threads in the coming revolution, the stakes for cybersecurity functions, and an updated CISO radar. This tool is widely used by Wavestone and its clients to support strategic thinking, for example, when developing master plans, holding collaborative seminars with employees to construct a specific radar for a company or business area, or to identify innovative solutions to be tested through demonstrations.

This publication presents the CISO radar and offers an overview of the areas we have identified as being key for 2019, from the 120+ topics the radar covers.

AUTHORS

GÉRÔME BILLOIS
gerome.billois@wavestone.com

DAVID RENTY
david.renty@wavestone.com

This publication was produced with contributions from Anaïs Etienne and all of Wavestone’s Cybersecurity and Digital Trust experts.

METHODOLOGY

The CISO radar is a tool that Wavestone has been developing and publishing each year since 2011. Three times a year, more than 40 experts meet to discuss the latest developments and key issues based on observations and experiences gained through working with Wavestone’s clients. The CISO radar covers over 120 subjects explored and analyzed by our experts. The radar contains a broad selection of the topics that CISOs must handle as part of their roles. It’s presented as a series of dials covering key themes (identity, protection, detection, risk management, compliance, and continuity) on three levels. The Mature level covers topics that every CISO can - and must - master. The Trending level covers topics currently being addressed; these are new areas where initial feedback can be shared. And the Emerging level covers topics on the horizon that are still little known or have no obvious solutions. These are included to better predict future developments and prepare for their emergence in companies.

Agility: faster, simpler, and more responsive

Large companies have begun their journey, or sometimes "forced march", toward large-scale agile operation. Faced with this transformation, CISOs must take ownership of these methodologies and work closely with development teams to grasp the challenges of cybersecurity. First, this coupling will enable security to be integrated into agile projects by means of Evil User Stories, security training for teams, the putting in place of continuous integration tools, and integrating intrusion tests into the development cycle. This journey is already well underway, with initial support projects proving successful.

Beyond integrating cybersecurity into agile projects, cybersecurity will need to turn the corner that agility represents by integrating itself into a new operating model. Not only will cybersecurity teams be involved in this agile structure by joining Feature Teams, giving visibility to CISOs on the risks identified in projects, but they'll also be able to provide security services in agile mode. Product Owners offering security services will appear—delivering "cybersecurity as a service" within organizations.

Cloud: multiple, automated, and secure by default

In 2019, the arrival of the first major deployments will trigger a chain reaction toward Cloud-First, or, for our most advanced clients, even Cloud-Only. Beyond applications, a nascent trend of infrastructure migration has begun, including for key components like Active Directories.

All these advances will involve a change in the role played by ISDs. Against this backdrop, CISOs will have to adapt to the new operating model to ensure the security of configurations over time and open dialogue with its new participants. They'll be able to encourage the use of new auto-remediation and system rebuilding capabilities in the event of a security incident.

This will require adaptations that provide a high level of control over rights-management administration and IS monitoring. In a context where the infrastructures are managed by the supplier, efforts need to be focused on these three key areas. Security will need to be integrated from the point of conception of new architectures and draw on the suppliers' bricks. Rights may need to be assigned in a more granular way to limit the risk of unauthorized access to resources. They will also have to be reviewed in automatic fashion to be adapted to frequent changes.

The cloud also represents a corner to be turned for security players, and CISOs will be on the front line in adopting—and making the most of—the market's offerings: vulnerability assessment, access control, MFA, Identity Governance, content filtering, etc. Many of these services are already available as credible cloud-based offerings.

In the medium term, multi-cloud, based on two providers, will need to be considered to assure the continuity of services.

API-fication: multiple new entry points to the IS

Driven by the PSD2 regulation in the financial sector, API-fication affects all sectors and enables services to interact by standardizing the means of data exchange.

We observe that all our clients' security functions are finding it difficult to master this new challenge. While API-fication can be a lever to facilitate the security of machine-to-machine exchanges through standardization, encryption and authentication, it presents a number of risks linked to the multiplication of APIs and the larger areas they expose. In fact, even major players like Google and Facebook are having difficulties in mastering this area, as incidents in 2018 have shown.

If CISOs want to take back control of the API-fication of services, they will, from now on, need to invest in this theater of operation using all existing means, including the most innovative ones. It won't be enough to simply define a governance approach or attempt, in the first instance, to inventory the exposed API; they must anticipate, and have the capability, to monitor and control large numbers of APIs.

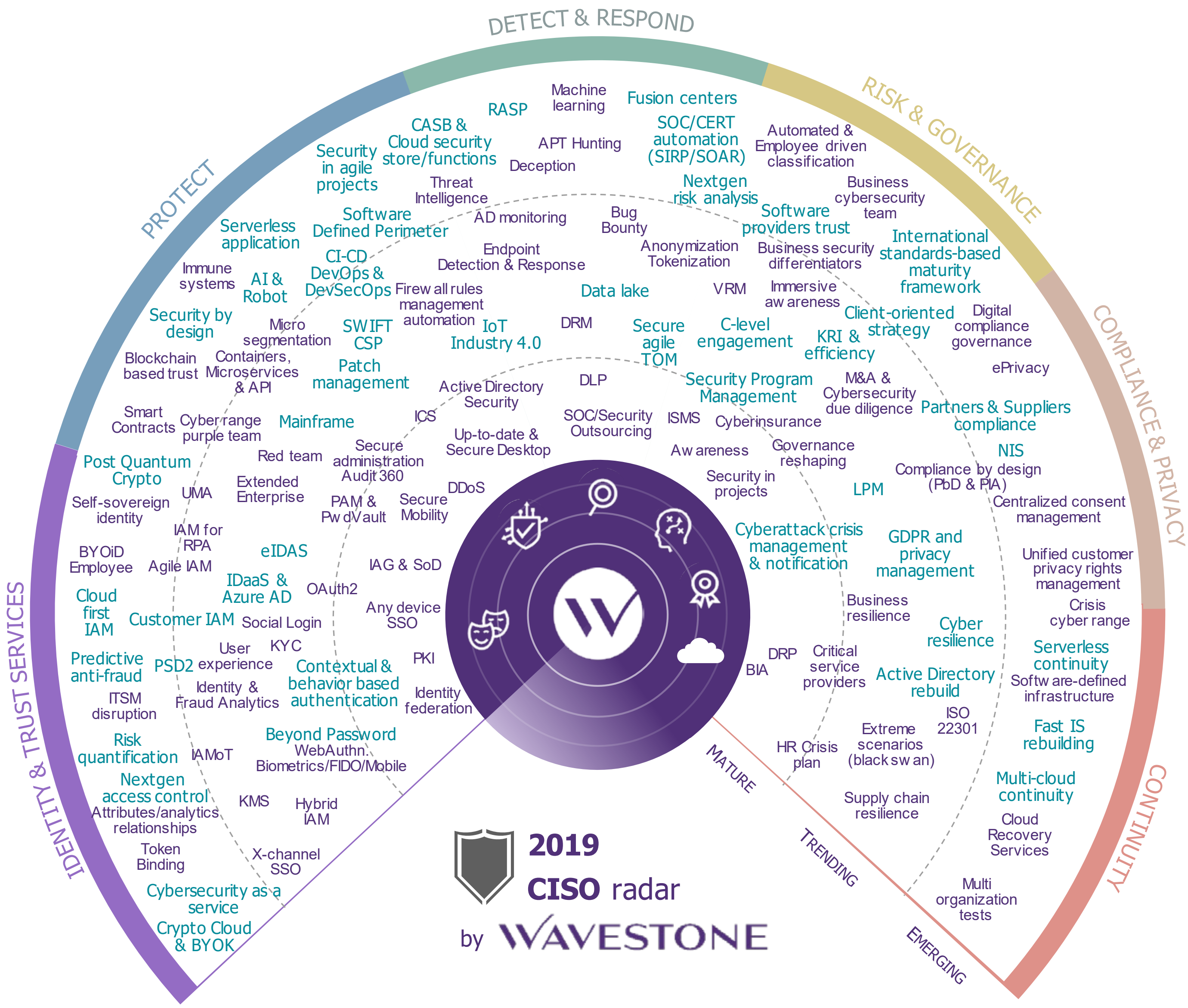
Si le RSSI veut reprendre le contrôle sur l'*API-fication* des services, il doit, dès maintenant, investir ce théâtre d'opération avec tous les moyens existants, y compris les plus innovants. Il ne pourra pas se contenter de simplement définir une gouvernance ou tenter, dans un premier temps, d'inventorier les API exposées ; il devra anticiper et être en mesure de surveiller et contrôler un grand nombre d'API.

A revision of the fundamentals

With a profound IS revolution taking place, ever increasing regulation in force, and penalties growing exponentially, how can security functions escape from the pressure cooker they find themselves in? To enable them to do this, we've identified two major projects that relate to the fundamentals:

/ **Overhaul the ISSP and governance.** These will need to be reviewed on the basis of the existing security strategy. To accelerate and provide a framework for the process, CISO's can draw on the NIST Cybersecurity Framework, a voluntary US framework that is becoming essential to large groups in all sectors;

/ **Conduct an in-depth review of the processes for integrating security into projects.** After being modified in 2018 to meet the needs of the GDPR, these will have to be reconsidered to increase agility and flexibility. The authorities are playing their part in this trend, with ANSSI (the French National Cybersecurity Agency) modernizing the EBIOS risk analysis methodology, recently named EBIOS Risk Manager, through an approach that combines compliance and attack scenarios.



BEYOND OVERHAULING THE FUNDAMENTALS, HERE ARE OUR FIVE PRIORITIES FOR ISS FUNCTIONS

- **Cloud-based cyber-resilience: the evolution of offerings enables the consideration of the cloud as a continuity solution against cyber-attacks, as is already the case for emails.**
- ***Fusion Centers*, the future SOCs: these will bring together both technical and business know-how, enabling an end-to-end understanding of possible fraud or intrusions into the IS, and to respond in the best possible way.**
- **The end of passwords: initiatives such as the 0-password, the deployment of FIDO2, the use of biometrics within a 2FA framework, or the broader roll out of safes, can be considered here.**
- **AI and *machine learning*: these technologies represent opportunities in the medium-term. The priority for 2019, however, will be to ensure that specific risks and vulnerabilities (inference, poisoning, etc.) are taken into account in business projects that make use of AI.**
- **Third parties and suppliers under the microscope: many of the attacks taking place today are being observed by suppliers. However, this doesn't make them any less damaging to the client company's reputation. There's a need then, in 2019, to better map interactions with providers in order to assess their levels of security. This is a complex task, given their number, diversity, and interconnected nature.**

EMERGING AREAS

Anticipating and adapting to the ongoing shortage of talent

There's no magic solution here, rather a range of options to be tested in order to cope with the skills shortage. From a technical standpoint: automation, cloud migration, and establishing a strong framework that puts in place security-by-design principles, will help to limit the effort required. Similarly, the creation of security-services offerings, both nearshore and offshore, for standardized services can provide solutions.

To meet tomorrow's challenges, CISOs will need to foster a new dynamic in the security function by creating a stimulating, ambitious, and educative environment that empowers teams. Their objectives will need to be the creation of new vocations and a desire for internal mobility.

Making security a differentiator for the company's customers

Security has often been considered a constraint. In 2019, it will no longer be enough to view security as an essential line of defense deployed across all companies: instead, it must be seen as a value generator for the core business.

This change affects almost all business sectors. The banking sector is moving down this road with the implementation of dual authentication systems, dynamic cryptograms, notifications in the event of suspicious transactions etc. and other sectors will have to quickly follow suit:

/ The automotive sector, with 'visible' security for connected vehicles, before it can move on to the autonomous vehicles of tomorrow;

/ Telecom operators, some of which are promoting new 'hubs' that incorporate cybersecurity services such as vulnerability detection;

/ Service providers to the general public (transport, energy, water, etc.) where cybersecurity is required as part of the sales process and can be a differentiator.

So, with CISOs leading, security functions must seize these opportunities to get closer to the business and demonstrate what they can offer at the heart of the organization's activities. Leading players like Apple have adopted this approach by putting security and privacy at the center of their value propositions.

We hope that this example will be developed further.

WAVESTONE

www.wavestone.com