THE CISO RADAR

ANTICIPATE TO BETTER PRIORITISE

What priorities can be identified from today's raft of cybersecurity topics?

Cybersecurity is constantly evolving, with new technologies and innovative solutions emerging every month. Faced with such rapid development, it can be difficult to spot the underlying trends and steer your cybersecurity strategy accordingly. Since 2011, to keep abreast of this rapidly changing world, Wavestone's cybersecurity experts have been meeting regularly to discuss market trends and identify core issues, news topics, and emerging technologies to be explored. This work has enabled us to build the CISO radar. It aims to support cybersecurity managers in taking a step back, and positioning and prioritising their actions amongst the wealth of cyber-related topics clamouring for attention. Wavestone and its clients use this tool widely in strategic thinking activities such as creating masterplans, collaborating with colleagues to build a company or domain-specific radar, or identifying innovative solutions to be tested through demos.

This publication presents the radar and offers an excerpt from the topics we have identified as being key for 2018, among the 130 live topics in the CISO radar.

METHODOLOGY

The CISO radar is a tool that Wavestone has been developing since 2011. Three times a year, more than 35 experts meet to discuss the latest developments and key issues, based on experience gained with the clients we support. The CISO radar looks in detail at more than 130 issues identified and analysed by our experts. The radar contains a wide selection of topics that CISOs must handle as part of their activity. It is organised into dials representing key themes (identity, protection, detection, risk management, compliance, and continuity) on three levels. The Mature level presents issues that CISOs can—and must—master. The Trending level presents issues that are currently being addressed; these are new areas where first feedbacks can be shared. The Emerging level presents future issues, about which there is still little known, or for which there are no obvious solutions. These issues are identified to anticipate future developments in the best possible way, and to prepare for them to be taken up by companies.

AUTHORS

GÉRÔME BILLOIS
Gerome.billois@wavestone.com

DOMINIQUE YANG
Dominique.yang@wavestone.com

This publication was produced with the contribution of Wavestone's cybersecurity and digital trust experts.

KEY CURRENT ISSUES

CUSTOMER-oriented strategy

Digitisation, disintermediation, disruption... it's never been easier for customers to switch vendors. They must be regularly persuaded to adopt new solutions, and their trust becomes a key asset in companies' digital transformation. Moreover, customers are paying more attention to cybersecurity, awareness is raised by repeated incidents reported in the media, or by regulatory changes that remind them of their data rights (access, security, portability, etc.).

Cybersecurity managers' responsibilities must thus go much wider than simply their infrastructures and their data. More and more, they need to focus on their company's customers. It's about evaluating their security expectations and offering them the functionality that ensures the security of the data they hold—simply and efficiently.

This change of emphasis requires CISOs to take a new step further—understanding their company's customers. The most innovative approaches we have observed include conducting customer surveys to understand expectations and explore potential new services. Or the integration of security services into the company's offering, with or without an additional charge.

It's important that CISOs are rallied to help shape customer journeys and sales pitch, and then play their part with a rationale that facilitates customer experience—not just with a strict security approach. CISOs from digital service providers have often taken the lead here! They've been dealing with their customers' questions, as part of tendering processes, for a long time, something that is not the case in many other sectors.

Adopting a client-centred strategy demonstrates, in practical terms, what the IS security sector can bring when providing new services and protecting clients' interests.

Cyber-resilience and Fast IS rebuilding

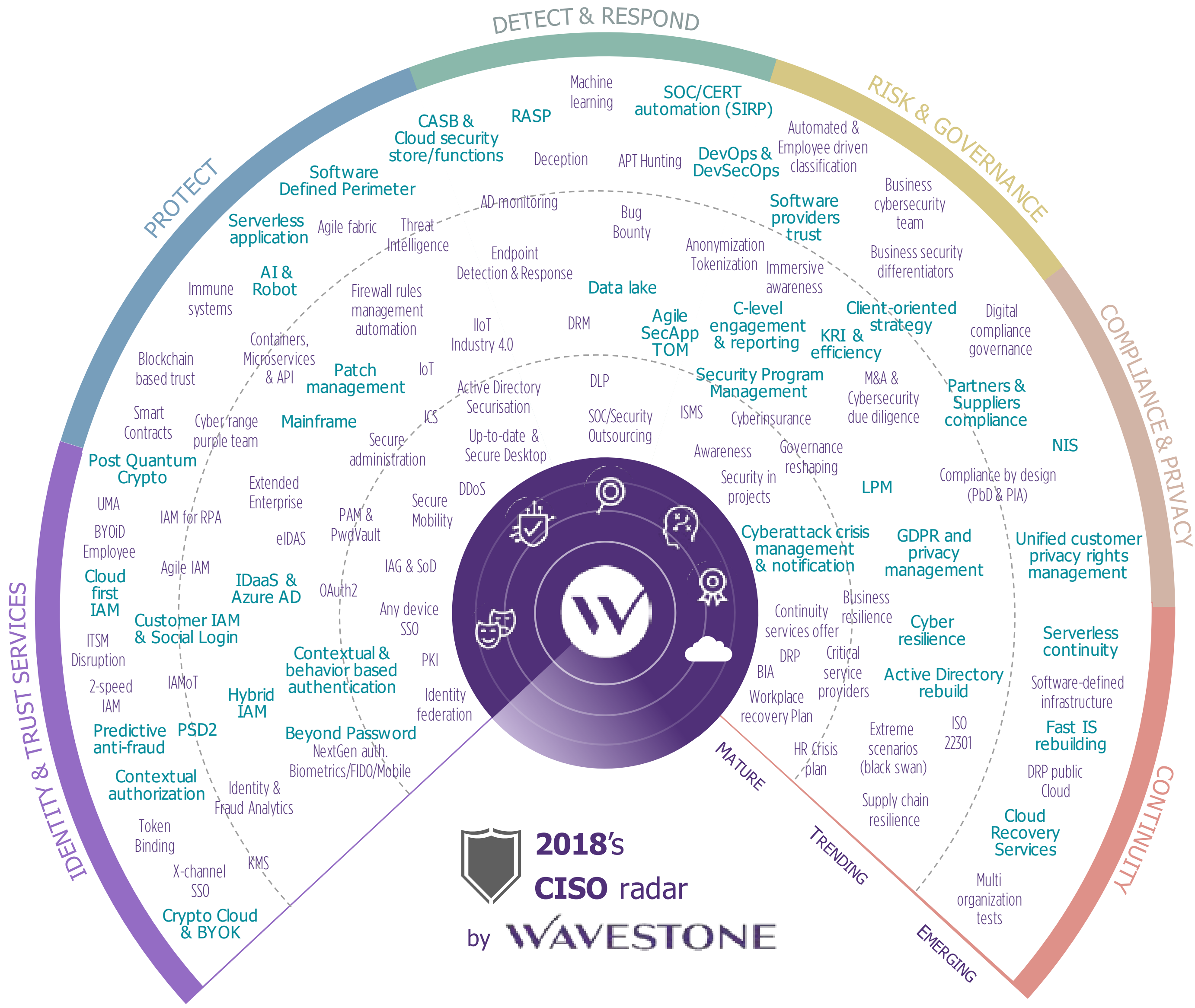
Wannacry and NotPetya have shown the ability of malware to destroy entire chunks of information systems within hours, with the impacts on the businesses affected running into hundreds of millions of dollars. Destructive threats like this were often considered hypothetical until this point. 2018 should be the year in which large companies clearly define their cyber-resilience strategies. There are two main types of activity to be considered. The first aims to limit the occurrence of this type of attack by ensuring basic security hygiene and particularly by addressing in depth the always complex **Patch Management** topic. The aim is also to secure suppliers (**Partners and Suppliers Compliance**). It's important to note that NotPetya was initially able to spread through the hacking of a third-party software provider (MeDoc) which became a Trojan horse to successfully enter the information system (**Software Providers Trust**). This is an attack technique that must be considered today in threat assessments. The second type of activity aims to determine how a crisis of this type should be managed, and, in particular, to prepare to rebuild an IS—very quickly—in the case of a successful attack (**Fast IS rebuilding/AD rebuild**).

Compliance: GDPR, LPM, NIS, PSD2

2018 will mark a turning point for compliance, with the entry into force of a raft of new legislation, including the General Data Protection Regulation. Beyond the GDPR and sector-specific legislation like **PSD2**, it is the arrival of the **NIS Directive**, its transposition into European member state-specific law, and the future identification of Operators of Essential Services (OESs), in November 2018, that will pick up the regulatory baton. This topic, subject to a pan-European measure, but implemented individually by Member States, may also have a significant effect on where some digital-service providers locate themselves. With the potential for requirements and security rules to be different between European countries, it's important that a "cybersecurity-dumping" scenario does not develop. In France, OESs already identified as Critical Infrastructures Operators (OIV), under the French **LPM**, should be less affected. In fact, the **LPM** already imposes a range of demanding requirements (including areas historically left out such as **Mainframe** security), and the current actions needed to meet them are not expected to be duplicated as part of NIS-Directive compliance. However, it should be noted that the directive's scope is likely to be wider than that of the **LPM**, and this may result in the addition of new systems located in secure zones.

Artificial intelligence

Artificial intelligence was, without doubt, the buzzword of 2017. But, out in the field, **Machine-Learning** technologies are in the process of proving their worth - and generating tangible results. This is particularly true in the fight against fraud on digital channels (**Predictive Anti-Fraud**). Given the volumes and responsiveness requirements, these technologies (**Data Lakes**) can provide solutions when conventional methods reach their limits. Authentication is another area that can benefit from these advances, with the implementation of biometric systems (**Beyond Password**) and/or those that dynamically adapt requirement levels according to users' actions (**Contextual and Behaviour-Based Authentication/ Contextual Authorisation**). However, these technologies are not yet fully mature for cybersecurity surveillance, although 2018 is expected to see major breakthroughs. And, without waiting for fully automated solutions (**SOC CERT automation**) to appear, carrying out initial tests on the role artificial intelligence might play in the management and resolution of incidents can help to understand the breadth of the issue.



C-level engagement and reporting

2017 marked a real change in the relationship between cybersecurity functions and executive committees. In nearly 25% of CAC 40 groups, ambitious security programmes are being implemented—with investments running to more than €50m (**Security Programme Management**). These programmes are being monitored directly by executive committee members. This is a real change of approach for the IS security sector, which, in 2018, will need to demonstrate the effectiveness of the programmes funded by these budgets (**KRIs and efficiency**). And, against a situation where competence is scarce and talent must be retained, it's no simple task; it's also one where, as soon as one threat is addressed another appears, and where strategies can be called into question if a major incident occurs. A high degree of willingness to raise awareness and to demonstrate that risks are under control are required here. For those who never spoke to the C-suite, the current climate has never been more suitable to put the topic in the spotlight. There's no doubt that the high-profile incidents increasingly being reported in the media, along with their major financial impacts, are helping to fuel this change. But it's mostly investments being made by other large corporates that are acting as the trigger. 2018 will be an opportunity for many to set up real programmes and secure the budget needed to transform cybersecurity.

Cloud

The use of cloud services is now a reality. SaaS is widely used and requires—beyond the essential trust in the provider—thinking about the security of privileged accounts, identity management, user access, and data sharing. **Cloud Access Security Brokers** (**CASBs**) can help cybersecurity managers to gain visibility on the services being used, and how to better secure them. While **CASBs** are emerging, they tend to draw closer toward **IDaaS** (**Azure AD**) solutions, where identity and access management is managed, or co-managed, in the cloud. It is also referred to as **Hybrid IAM** and **Cloud First IAM**. On the other hand, cloud deployment is now moving toward IaaS, with the growing use of Amazon and Microsoft solutions, among others. Their implementation requires a thorough overhaul of security models and thinking about emerging issues, such as the **Crypto-Cloud**, which embodies the **Bring Your Own Key** principle, or **Cloud Recovery Services,** which harness the cloud for cyber-resilience purposes by providing a cloud-based continuity solution, should applications become unavailable.

THE EMERGING TOPICS TO TRACK

Serverless/Serverless Continuity

Serverless is a new cloud paradigm that sits between IaaS and SaaS, close to PaaS, and aims to offer the capability to publish code directly on cloud platforms without having to worry about operational maintenance and the maintenance of the security of underlying infrastructures: developers no longer have to worry about server provisioning or operating-system-level access. This paradigm shift must be monitored by operational security teams to adapt their procedures and analysis, in order to ensure that cloud service providers offer the appropriate level of security, particularly in terms of monitoring the systems. In fact, if anything, they make surveillance teams just that little bit more blind. The question of business continuity—**Serverless continuity**—is also important. There is a need to rethink business continuity capabilities in an environment where the customer no longer has control over system-level backups, and where continuity needs to be application based or cross-platform based.

Runtime Application Self-Protection

RASP is a security technology that is built into an application or runtime environment that aims to detect attacks and protect the application, in real time, via dynamic analysis. **RASP** enables security to be placed in a higher layer, closer to the application and its data. This technology is being developed by start-ups such as Canada's Immunio (which was recently acquired by Trend Micro), Tcell or Prevoty in the United States, and Sqreen.io in France.

Unified Customer Privacy Rights Management

Beyond introducing the concept of portability, the European regulation also reinforces requirements on consent collection. These two aspects can be addressed by **Unified Customer Privacy Rights Management,** which, in particular, translates into a single platform, or interface, for access to customers' personal data. These emerging solutions must be monitored in parallel with **Customer IAM** (**CIAM**) platforms, which can provide richer functions.

Software-defined Perimeter & Automation

Software Defined Perimeter (**SDP**) is a set of security technologies that introduce agility and automation into security. The rise of cloud and agile accelerates deployment cycles and the deprovisioning of systems or services, sometimes even in real time. These developments mean that security must keep pace. By introducing automation and adding more granularity to IS segmentation, **SDP** provides access only to the necessary resources required for a service to function, or for the user to perform the desired action. Examples of early initiatives include Google's "BeyondCorp" and the joint effort of the Cloud Security Alliance and the start-up Vidder.

Post Quantum Crypto

Post Quantum Crypto is representative of the new technical solutions for encryption that must be considered to anticipate the increasing maturity of the quantum-computing capacities that will make cryptanalysis possible on encryption algorithms, such as RSA, which are considered robust today. The major internet players, like Google and Microsoft, are starting to take an interest in the subject too, carrying out early work on encryption algorithms that are resistant to quantum attacks. The NIST began work in the area in 2016, and hopes to publish its first drafts by 2023-2025.

WAVESTONE

www.wavestone.com

Wavestone is the result of a merger between Solucom and Kurt Salmon's European operations (excluding consulting in the retail and consumer goods sectors). It is a leading independent player in European consulting.

Wavestone's mission is to enlighten and guide its customers in their most strategic decisions by applying its triple functional, sectoral and technological—expertise.