Factsheet

protecting your organization from the unseen enemy in cyberspace

Cyber protection from battlefield to boardrooms

The world around us is changing. Organizations are becoming more aware of the delicate balance between the potential benefits of emerging technologies and the possible threats associated with them. Keeping the enemy out is old thinking, because securing all processes 100% is unaffordable. So how can defence, security and other key agencies protect their critical assets in the cyber ecosystem?

Managing threats in the cyber ecosystem

Cyber attacks can use limited and commonly available resources to wreak great damage, which is why they are an asymmetric threat. Whether hostile nations, terrorists, 'hacktivists', or organised crime... it's usually extremely difficult to assign attribution of a cyber attacker, because the open nature of the internet allows an attacker to spoof their IP address and obfuscate their identity by routing through a series of proxy servers or by utilizing a botnet.

The result of an attack can be severe for any organization, not only in terms of the financial loss, but also in damage to reputation. This is damage that can be difficult to repair, and broken trust can take even longer to rebuild. For key organizations such as defence, security and critical national infrastructures (CNI), attacks can also result in physical harm to individuals.

No agency is safe from attack, and past experience is no protection. The Pentagon experienced one of the first ever cyber attacks in 1998, but 10 years later, it still became a victim of a malware attack with an infected USB-stick. This event is believed to be the cause of the biggest cyber attack on the US Department of Defense (US DoD), involving significant amounts of classified intelligence sent to a foreign intelligence agency. It took the US DoD more than 14 months to clear the malware from its systems.

The most successful vectors of cyber attacks always focus on the weakest link of a critical end-to-end process. This vulnerability might be inside your organization, but it might also be in another organization connected to you, such as the supplier of your software, security certificates, or communications and hardware equipment. Because of this vulnerability, the trend is away from organizational cyber protection and towards cyber protection of critical processes across the entire cyber ecosystem. (The cyber ecosystem is global and includes government and private sector information infrastructure; the variety of interacting persons, processes, information, and communications technologies; and the conditions that influence their cyber security[1])

[1] Definition taken from US Department of Homeland Security, "Blueprint for a cybersecure future: the cybersecurity strategy for the homeland security enterprise" (2011)

Protecting your organization from the unseen enemy

Cyber threats are everywhere: USB sticks, smartphones, botnets, distributed denial of service, identity theft, social engineering, data exfiltration – even the information employees post on social networks can make you vulnerable.

Achieving full cyber security requires information superiority. It is essential to deliver the right information, to the right person, in the right format, at the right time. In short, network enabled capabilities, and information centric warfare are not only needed in the traditional domains of land, sea, air and space. They are just as important in securing the fifth domain, the cyber ecosystem, and require the same capabilities with the same holistic approach.

The only cyber security is holistic cyber security

Atos can help you create this holistic approach to cyber security. Only by integrating cyber defence, identity management and secure collaboration can an organization really secure its critical assets. Atos works with an architecture that enables you to really get to grips with the threat you face. Our central belief is in the value brought by an **integrated risk management approach**. We use attack models, risk assessments and an understanding of vulnerabilities to ensure the best outcome for a security project.

As a founding member of the European Organisation of Security (EOS) and the International Cyber Security Protection Alliance (ISCPA), Atos can ensure protection of all critical information in your processes.

Defending your systems from external threats

Defence and security organizations implement emerging technologies to enable more cost-effective ways of making their services available. This results in a **greater use of online technologies**, such as self-service applications, remote log-in facilities, and cloud-based business models. This extended use of technology and increased connectivity also means a greater risk of a cyber attack. Atos offers solutions drawn from the technology developments of our Atos Research & Innovation group, the expert knowledge of our global partner alliances, and best practices used by our clients to provide an extensive knowledge of **workplace security** and **critical infrastructure security** – delivered with a zero-risk approach.

Protecting against the insider threat

A malicious insider threat to an organization can be a current or former employee, contractor, or other business partner. He or she has now, or has had in the past, authorized access to an organization's network, system, or data, and has (misused that access, intentionally or not. The complexity of today's technology increases the chances that accidental user error can leave systems **open to external attack**.

There is still a lack of awareness of cyber security amongst the workforce in many organizations. Examples are the amount of classified information published on open social media, or the inadequate passwords that people use. Atos delivers fully integrated **Governance, Risk Management and Compliance** processes with a large suite of solutions on cyber intelligence, (biometric) identity management and forensics to protect both the organization and its users. Together with awareness training, we bring cyber security from the battlefield straight to the boardrooms, making security part of your company's DNA.

Secure cooperation with partners

Cooperation with partners is changing. In the cyber ecosystem the number of partners is growing fast, and the amount of data – often big data – moving back and forth is also increasing. The cloud holds part of the answer by keeping all data in one place. But even so, the dangers associated with partner interfaces have been considerately **underestimated** so far.

Cyber security solutions to this problem need to include communication networks, high encryption technologies (such as those developed by Atos Worldline), and deliver high security for specialized clouds.

Atos as a trusted partner in your Cyber Ecosystem

Organizations need to choose a proven leader in the security solutions marketplace. Atos has worked with defence and security organizations around the world, enabling core business operations and helping agencies to minimize the risks of cyber attack. Atos has won the European Identity Management Solution of the year award three years running from 2010 to 2012, and the international 'red dot design award 2012' for its latest hardware security encryption module.

We have more than 500 cyber security experts and several hundred business technologists working within defence and security organizations with specific knowledge of the defence and security sector,

Atos is the worldwide IT technology partner of the Olympic Games and it provides the IOC with the comprehensive cyber security system for the Olympics. Using the latest cyber technologies, no critical incident affected the London Olympics and Paralympics. Part of that success lies in early preparations. Therefore, our security preparations for the Olympics in Sochi and even Rio de Janeiro are already underway.

Whatever your role in the defence or security world – military, intelligence, governmental, emergency service or border control – Atos cyber security solutions can protect you from the unseen enemy.

For more information, contact: cyber@atos.net

atos.net/cybersecurity