Arthur D Little

Viewpoint

ICT security in the digital transformation era

Do organizations need digital security strategies?

The rise of digital transformation and cyberspace, as a result of the Internet of Things (IoT) and Industry 4.0 spreading, will increase the risk of cyber-attacks. Public and private organizations need to define strategies, organizations, processes and how to manage the information capable of mitigating cyber threats, while remaining aligned with security, confidentiality and traceability requirements for compliance with recent regulations.

The digital security need

Digital transformation is radically changing society and the international economy, favoring new political and social interactions, as well as new economic and commercial transactions. New technologies and initiatives, such as the Internet of Things (IoT) and Industry 4.0, are leading the evolution of "net" use, introducing new users and increasing the quantity and the types of data. The process of network-access cost reduction and the increasing diffusion of broadband will boost internet traffic in the next years: high growth rates been 2015 and 2020 are expected everywhere, with peaks of more than 40 percent in the Middle East and Africa. Cisco foresees a monthly worldwide increase, from 88.7 exabytes in 2015 to 194 exabytes in 2020 (CAGR 17 percent). The adoption of new digital technologies is increasing the cyberspace and, consequently, related risks.

The cyber risk

Cyber risk is the operational risk associated with organizations' economic losses caused by data and/or information systems being unavailable, lack of integrity or confidentiality failure. Its origin can be accidental (e.g., shutdown of a server) or intentional (e.g., theft of sensitive data). In the latter case, cyber attacks represent the main threat: mainly automated actions designed to disrupt, damage or hamper normal system operations, networks or processes. Various potential consequences can be caused by a cyber-event that is either internal or external to the organization, such as interruption of activities, reputation/image damage, dissemination/violation of confidential data, violation of intellectual propriety and legal actions. Cyber-attacks are carried out using "cyber weapons": malicious software (abbreviated "malware") specifically designed to damage or modify an information system.

The WannaCry Virus

The biggest cyberattack in history took place on 12th May 2017, when thousands of information systems were paralyzed. The WannaCry virus, responsible for the attack, encrypted the targeted hard disk and did not allow users to access their data. Victims had to pay a ransom to retrieve the information contained on the hard disk: ransoms were up to $600 for each machine. Over 150 countries were affected, as well as at least 40 main industrial groups, for a total of about 300,000 victims. The ransomware struck only out-of-date information systems: **better digital security management and organization could have prevented the attack.**

The main cyber attackers can be classified by the following categories:

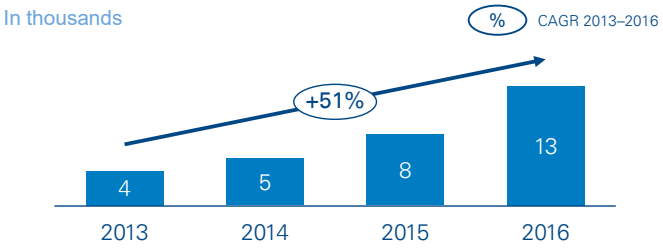
- **Financial:** Financial motivation or organized criminal group actors
- **Espionage:** Espionage motive or state-affiliated or nation-state actors
- **FIG:** Fun, Ideology, Grudge motives, or activist-group threat actors

Threat evolution and impact

The number of computers targeted by ransomware in 2016 is remarkable: according to Kaspersky, 32 percent of machines were subjected to at least one malware-class web attack, and around 1.4 million computers were targeted by encryptors. Worldwide ICT security did not have an easy year. Several incidents appeared on newspaper pages, highlighting the limits of the existing infrastructures and issues linked to traditional IT security management.

Analyzing Verizon 2017 and 2016 reports, a 26 percent increase of incidents in the private sector emerged. (An incident is defined as a security event that compromises the integrity, confidentiality or availability of an information asset.) The sample does not represent all data breaches in all organizations, but it gives a clear view of the observed phenomena.

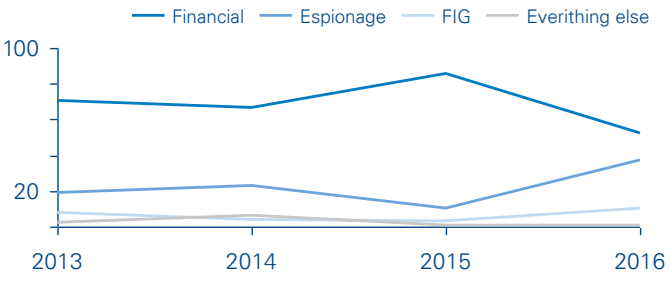
Incidents trend in private sector



Source: Verizon – Data Breach Investigations Report – 2017, 2016, 2015, 2014, Arthur D. Little

The number of incidents in the private sector is critically growing, having more than tripled in 2016 compared to 2013. In 2016, 90 percent of incidents were committed in manufacturing, professional, healthcare, entertainment and finance; there was an increase in the first two by more than 200 percent compared to 2015.

% distribution of aggressors

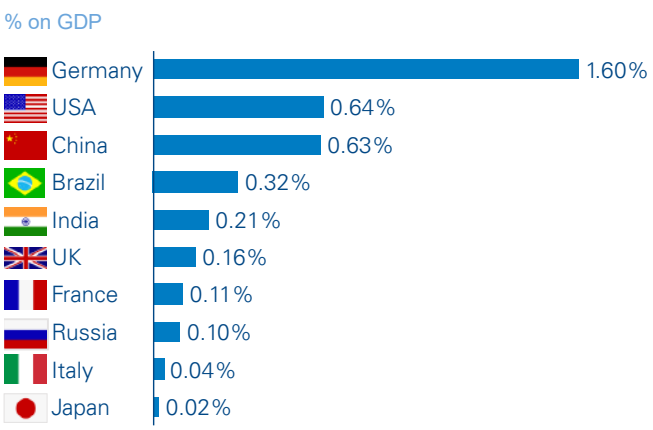


Source: Verizon – Data Breach Investigations Report – 2017, Arthur D. Little

Regarding the distribution of the aggressors, the first motivation for aggression was financial, but the total of these fell in 2016; espionage significantly increased in 2016 to the highest level ever.

Consequently, this huge amount of aggressions has a strong economic impact: the total cost estimation hovers around $450 billion globally. Considering losses in GDP, Germany is the first country, followed by the US and China.

Estimated losses derived from cyber-crime

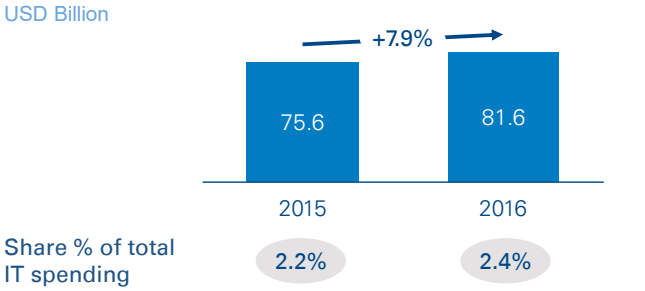


Source: Allianz 2015; Arthur D. Little

IT security spending

Organizations are spending more money to protect themselves against cyber-threats: the total worldwide investment in products and services for information security reached about $82 billion in 2016; its growth rate was higher than total IT spending, which demonstrates companies' sensitivity to the issue. Despite the increased expenses, however, it represents only 2.4 percent of total IT spending.

Worldwide IT security investments



Source: Gartner - Forecast Alert: IT Spending, Worldwide, 1Q17 Update, Gartner - Forecast Analysis: Information Security, Worldwide. Arthur D. Little

The growth of IT security investments will maintain the same in the next years: its CAGR is forecast to be about 7.9 percent through 2020, much higher than the 2.5 percent CAGR of overall IT spending.

The growth of IT security investments will maintain the same in the next years: its CAGR is forecast to be about 7.9 percent through 2020, much higher than the 2.5 percent CAGR of overall IT spending.

1 In the analysis, the private sector is the aggregate of the following sectors: accommodation, administrative, agriculture, construction, education, entertainment, finance, healthcare, information, management, manufacturing, mining, professional, real estate, retail, trade, transportation, utilities, other. This does not include incidents in public and unknown target sectors

The pillars in the European regulatory framework

	GDPR REGULATION (Regulation EU 2016/679)	NIS DIRECTIVE (Directive EU 2016/1148)
GOALS	▪ **Protection and management** of citizens' **personal data**	▪ Build a common and high network and systems security level among European states
SCOPE	▪ **All organizations** dealing with personal data in EU territory	▪ All **operators of essential services** in critical sectors **(energy, bank and financial market infrastructure, transport, health, supply/distribution of drinking water, digital infrastructures)** ▪ **Digital services providers** with at least 50 employees and annual balance sheets of more than 10 million euros
MAIN ELEMENTS	▪ Protection and management of natural person's personal data ▪ Management of personal data as a process impacting the whole organization of the company ▪ Protection of privacy, starting from the first design phases (**Privacy by Design**), aiming at inherently safe and non-vulnerable solutions, and ensuring that only necessary personal data is managed by default (**Privacy by Default**)	▪ Improve cybernetic security architecture for every single member state, creating a common management system on EU territory ▪ Favor information sharing, enhance cooperation among EU states to better deal with transnational cyber crime ▪ Improve the company structure (operators of essential services and digital services providers) to monitor risks and manage attacks
DUTIES	▪ Definition of data storage times and indication of origins of data in case of use ▪ Inform authorities when a database violation occurs ▪ Establish the evaluation impact document of management of personal data ▪ Manage the accountability in the field of data protection with adequate organizational structures (mainly with **Data Protection Officer**)	**For member states:** ▪ Establish **CERT** ▪ Establish one or more relevant national authorities expert in the field of network security and information systems ▪ Create and maintain a list (updated every two years) of all operators of essential services **For operators of essential services and digital providers:** ▪ Introduce "adequate and proportionate" security systems and teams able to deal with cyber-attacks ▪ Communicate accidents at the authority ▪ Test and certify networks and information systems resilience capacity. Their systems should be designed to prevent and reduce the impact of accidents and ensure the essential services (Security by Design)
TIMELINE	▪ It will be applied from 25th May 2018	▪ Transposition until May 2018 for every European member state

Source: Arthur D. Little

The regulatory framework is complex, and composed of a European regulation and directive. The legal basis includes:

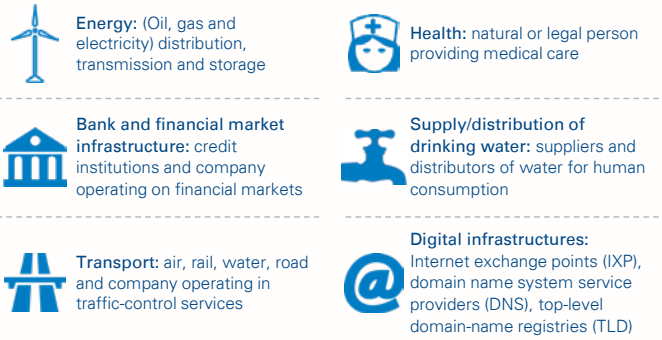
- **The General Data Protection Regulation (GDPR):** This contains the norms for natural persons, and specifically the processing of personal data.
- **Network and Information Security (NIS):** This contains the measures regarding the definition of a common high security level for networks and information systems for EU countries.

GDPR compliance requires companies to equip themselves with specific skills related to identity and data management; in fact, the regulation provides precise professional roles, including Chief Security Information Officer (CISO) and Data Protection Officer (DPO).

According to a Dell Survey, European companies' readiness regarding the GDPR is low: 36 percent declared that they are not prepared, and 27 percent do not know if they are. Looking at how companies are moving to comply with regulations, a serious issue emerges. Only a small group of companies (3 percent) own clear plans. The majority are working on the development or figuring out who has to be involved (37 and 27 percent, respectively). The remaining companies (33 percent) have not started yet.

The Cooperation Group, composed of representatives of member states, Commission and ENISA, started its activities in February 2017. The first milestone was in August 2017, when digital service providers had to adopt the security requirements and the system for notification of incidents. Member states still have time to meet their obligations; some have already transposed part of the NIS directive into their legal systems. For example, Italy has defined its national cyber strategy. EU countries have until November 2018 to identify the operator of essential services in critical sectors.

Critical sectors of essential service operators are



Source: Arthur D. Little

The NIS directive will reach full implementation in 2021, when auditing regarding the correct NIS implementation, with

particular focus on strategic cooperation among states, takes place.

Conclusion

Digital transformation will continue to increase cyber threats, seeking innovation and transformation of security management. Risks of huge economical and image loss are leading private organizations to increase their awareness regarding the importance of processed information and related protection for achieving business goals. On the other side, public services mainly implement organizational and technological security safeguards due to regulatory compliance.

Compliance with upcoming regulations is necessary, but not sufficient; any corporation can be breached due to human ineffectiveness/negligence. It is outmost importance to understand that no matter how robust the technology is, a single instance of human carelessness may cause its fall. A corporate culture respectful of digital security is the greatest defense a corporation can set up to protect its digital environment. Technical solutions can only do so much to make up for human negligence.

The real question is, how can a company know that it is safe from such threats? What can be done from a practical point of view?

The building blocks of a good cyber-security strategy are:

- **Organization, processes and governance:** Definition of a security and privacy strategic plan and a governance model. Review of security and privacy processes and procedures.
- **Technical Management:** Simulation of attacks to identify vulnerabilities and areas for improvement. Identification and implementation of SW for prevention and response.
- **Cultural Management:** Communication and training in order to guarantee human/cultural propensity for adequate behavior.
- **Continuous improvement:** Introduction of security measures and proactive monitoring of processes and system performance.

Contacts

Austria
virag.bela@adlittle.com

Argentina
monzon.daniel@adlittle.com

Belgium
vanoene.frederik@adlittle.com

China
russell.pell@adlittle.com

Czech Republic
brabec.dean@adlittle.com

France
bamberger.vincent@adlittle.com

Germany
doemer.fabian@adlittle.com

India
srinivasan.srini@adlittle.com

Italy
nico.mario@adlittle.com

Japan
mori.yonoshin@adlittle.com

Latin America
casahuga.guillem@adlittle.com

Middle East
merhaba.adnan@adlittle.com

Netherlands
kolk.michael@adlittle.com

Nordic
harenstam.fredrik@adlittle.com

Norway
mackee.diego@adlittle.com

Singapore
ito.yuma@adlittle.com

Spain
ali.salman@adlittle.com

Turkey
baban.coskun@adlittle.com

UK
eagar.richard@adlittle.com

USA
beaumont.mitch@adlittle.com

Authors

Katia Valtorta, Dario Garante, Nicola Giannelli, Walter Sala, Marco Giani

Arthur D. Little

Arthur D. Little has been at the forefront of innovation since 1886. We are an acknowledged thought leader in linking strategy, innovation and transformation in technology-intensive and converging industries. We navigate our clients through changing business ecosystems to uncover new growth opportunities. We enable our clients to build innovation capabilities and transform their organizations.

Our consultants have strong practical industry experience combined with excellent knowledge of key trends and dynamics. Arthur D. Little is present in the most important business centers around the world. We are proud to serve most of the Fortune 1000 companies, in addition to other leading firms and public sector organizations.

For further information, please visit **www.adlittle.com**

www.adl.com/ICTsecurity