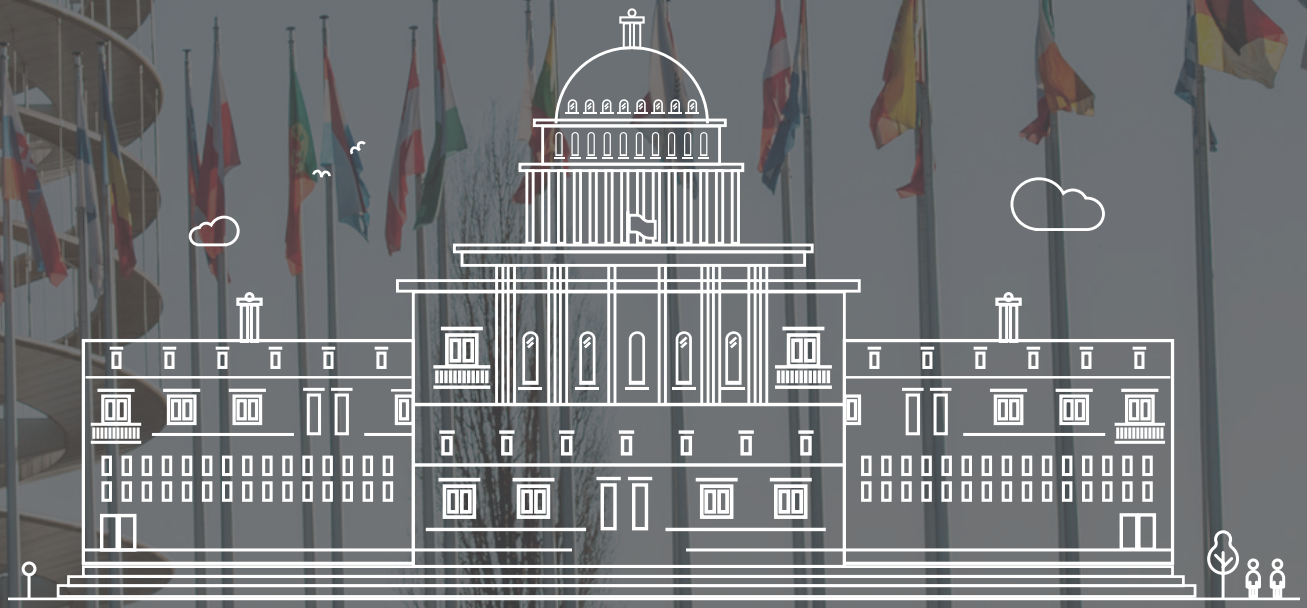
US Edition

Privacy in Public Administration



pandasecurity.com

panda

Technological Technocracy

The public sector is undergoing an unprecedented transformation as new technologies are now used across the board in all areas of the sector.

Implementing new technology is a key factor in improving processes and growing the economy. In fact, the level of governmental intervention in national economies has, in recent years, reached a new high. According to EUROSTAT, public sector spending in the EU has reached 48.2 percent, almost equaling the contribution of the productive economy. This underlines the extent to which our lives are influenced by public administrations.

Use of information and communication technologies in general and specifically, online government services, are key factors in the way the public sector is changing, as it delivers fast access to public services for both individuals and businesses.

However, **the adoption of new technologies by public agencies has also exposed them to new types of threats.** It is no longer sufficient just to look out for typical IT problems, such as prevention or reporting incidents. Now there is a real and ever-present threat of cyber attacks.

The best proof of this is the data provided by **the Government Accountability Office, which states that during 2015 a total of over 77,000 cyber attacks were detected in 24 federal agencies and companies of strategic interest. This figure represents an increase of 1300% over the year 2006.**

The technological revolution in the public sector, the digitalization and storage of information, and the boom in online services to simplify administration for the public have led to an exponential growth in the generation, storage and processing of confidential data; data which must be treated with the utmost care. Consequently, the public sector now faces a new series of demands in risk prevention, security and legal compliance.

Many public bodies have implemented new technologies without paying attention to these demands, and will now have to undertake a major effort to adapt to the new legal panorama.

The role of cyber-security

Cyber threats represent a constant and significant security risk for public administrations. So much so, that they have become a powerful weapon to attack the citizens and public agencies of countries. Such threats can seriously affect the quality of services and, more importantly, steal confidential information, from private data to state secrets.

Today's digital society is the main beneficiary of these technological advances, yet it must also use these resources responsibly and effectively. Cybersecurity is a key factor in improving user experience, complying with legislation and providing the protection needed by public entities.

Initially, the main purpose of IT security was to protect information reactively, but this then evolved towards a proactive approach, identifying and combating cyber threats, and has now given way to a Global Security Model.

Security, in any dimension or context, is the first responsibility of any government. Historically, security was managed by Defense departments, given that the main perceived threats to countries were of a military nature. In the present hyper-connected era, however, new players and risks have emerged that have forced governments to undertake major reviews and shakeups of their security and defense policies.

Such a shift is reflected in new legislation passed in recent years, as was the case with the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Gramm-Leach Bliley Act of 1999, and the Homeland Security Act of 2002. These laws marked a turning point in the use and management of communication technologies in the public sector, and its interaction with citizens and businesses, and between different national, regional and local governmental agencies. It represented a genuine regulatory, organizational, operational and technological transformation of the public sector.

Since then, in 2003, the President's National Strategy to Secure Cyberspace made the Department of Homeland Security (DHS) responsible for security recommendations and researching national solutions. The plan calls for cooperative efforts between government and industry "to create an emergency response system to cyber attacks and to reduce the nation's vulnerability to such threats". In 2004, Congress allocated $4.7 billion toward cybersecurity and achieving many of the goals stated in the President's National Strategy to Secure Cyberspace.

This new legislation brought increased attention to the NIST Enterprise Architecture Model initiated in 1988, the federal government of the United States promoted this reference model in the 1990s as the foundation for enterprise architectures of individual U.S. government agencies and in the overall federal enterprise architecture.

Cyber-attacks:

Data theft

Israel's Ministry of Social Security and Welfare

Over the last ten years we have witnessed all types of attacks against public administrations. One example, which took place between 2005 and 2006, involved Shalom Bilik, a computer systems maintenance contractor for Israel's Ministry of Social Security and Welfare. Bilik accessed a database and stole information pertaining to nine million Israeli citizens. The information was later sold and the theft went undiscovered until 2012, when Bilik and five other people involved in the processing and sale of data were formally charged.

Data stolen from 9 million Israeli citizens.

United States Department of Veterans Affairs

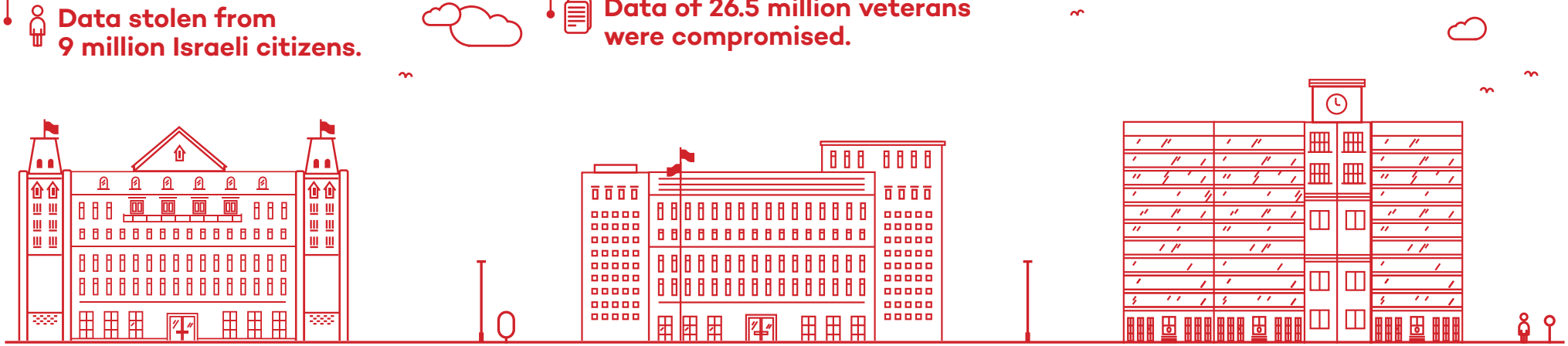
Not even our own homes are secure and even less so when it comes to the safekeeping of state documents. There is a lesson to be learned from the employee of the United States Department of Veterans Affairs whose house was robbed in May 2006, compromising the data of 26.5 million veterans, including their name, social security number and date of birth. The employee had been working on a statistical survey and had taken the information home without permission.

Data of 26.5 million veterans were compromised.

UK HM Revenue and Customs

Another case of the misuse of information occurred in 2007, was two hard disks from HM Revenue and Customs with the personal data of families with children under 16 in the UK were lost. Apparently, a courier firm had been entrusted with the disks, though they never reached their destination. The 25 million missing records included names, addresses, dates of birth and bank details.

Data lost of all UK families with children.



The White House

In 2015, Ben Rhodes, deputy national security advisor in the United States, confirmed that the White House had been the victim of an IT attack. In an interview with CNN, Rhodes acknowledged that the attackers gained unauthorized access to the unclassified computer system and stole key data. The classified system was not hacked.

The Office of Personnel Management

In June of the same year, it was reported that the Office of Personnel Management, the U.S. federal government's human resources agency, was compromised and the personal information of at least 4 million public workers stolen. The attack took place two months earlier, about the same time that the White House was compromised. Both attacks, however, appeared not to be connected.

Access to the unclassified computer system.

Access to personal data from 4 million of public workers.

Insiders

As was the case in many other sectors, most examples of data theft up until 2011 were inside jobs, carried out by employees with access to information.

Attacks from employees with privileged access are one of the greatest threats to the cyber-security of countries and businesses alike.

Whether it's a foreign spy, an employee kidnapped by terrorists or disgruntled employees simply stealing information out of spite, they are all insiders.

Bradley Manning

One of the most infamous data thefts of the modern era occurred in 2010, when Bradley Manning, a US soldier, copied 700,000 confidential documents and used WikiLeaks to publish the data.

In total almost **half a million records from the Iraq and Afghanistan conflicts, and more than 250,000 secret U.S. diplomatic cables.** Manning has consequently been charged with misconduct for violating federal laws on the disclosure of classified material, supplying intelligence to the enemy, breaching IT security and hacking security programs as well as espionage.

Edward Snowden

Another of the most notorious cases in recent years and one that had both the CIA and the NSA (National Security Agency) in a state of alarm featured Edward Snowden, a former employee of the latter, who in 2013 published top secret documents through the Guardian and the Washington Post, concerning various NSA programs, including the mass surveillance programs PRISM and xkeyscore.

The United States Department of Justice has determined Snowden's participation in the surveillance program PRISM as a "criminal matter", his fate is anyone's guess.

He copied 700,000 confidential documents.

Snowden published top secret documents, concerning various NSA programs.

Attacks against networks and systems

As technologies advance and systems become more interconnected, cybercriminals have more means and tools to carry out attacks, as has become clear thanks to the numerous cases occurred in recent years.

In 2012, a simple email message sent to employees of the South Carolina Revenue Dept. gave an attacker access to the internal network and the data of 3.8 million taxpayers. The stolen information included social security numbers and bank account details.

A similar attack took place in Monterey County, when the personal details of 145,000 residents were stolen by external attackers who managed to compromise a computer in the Social Services Dept. Once again, the data stolen included social security numbers, along with names and addresses.

An email message gave an attacker access to the internal network and the data of 3.8 million taxpayers.

Social security numbers and bank account details, were stolen.

Politically-motivated attacks

As the year 2015 witnessed scores of politically-motivated attacks against public institutions (including the hacking of social network accounts to spread propaganda), as well as spying on politicians and high-ranking officials.

Cyber-terrorism and cyber-espionage

Organized criminal networks (cyber-gangs) have begun to shift the focus of their activities towards cyber-space, taking advantage of the anonymity of the Internet in order to obtain sensitive information which can then be used fraudulently for financial gain.

In January 2015, just as Barack Obama announced a series of legislative initiatives to help in the fight against cyber-crime, a group of attackers with connections to ISIS seized control of the Pentagon's main social network accounts. To do so, they must have had access to details of email accounts, passwords, usernames, etc. Data and credentials that typically don't have the level of security necessary to prevent attacks and misuse.

Now terrorists and extremist groups are using cyber-space to plan attacks, publicize them and recruit supporters to carry them out.

This tactic was used by the group known as the Syrian Electronic Army, which managed to compromise the website of the US Navy, publishing propaganda in favor of Assad's Syrian regime.

The US administration once again became the target of cyber-criminals when James Comey, head of the FBI, told a security forum that they had detected a growing interest among terrorists in strategies for launching cyber-terror attacks against the United States. Without going into details about the type of attack, he said it appeared they were still in the early stages of planning and assessing how effective they might be. Nevertheless, this is potentially an issue that could have serious repercussions.

With the sabotage of industrial installations, assassinations of scientists and **the use of the Stuxnet computer virus, the secret phase of the war against Iran began during the last decade** with the spying by the US and Israeli intelligence services, who reached the conclusion that Iran had developed a uranium enrichment plant. This finally came to light in September 2009 after an announcement by Barack Obama.

Hacktivism

This movement really arose during 2011, when hacktivism became a serious threat to governments and public agencies. Its fundamental principles are anonymity and the free circulation of information across cyberspace, essentially through the Internet. Hacktivists have a decentralized structure, using underground networks to communicate and plan their actions.

The German parliament was the victim of an attack that compromised various computers and stole information from them. The attack is suspected to have come from Russia, although it is difficult to prove who was really behind the action.

On July 25, 2015, various Russian hackers were able to compromise the Pentagon's unclassified email system and steal information. According to official sources, it was the result of a highly sophisticated attack and was clearly engineered by a government.

Similarly, this year three groups of Latin American attackers managed to compromise the mail servers of the Bolivian army, downloading emails, some of which they published. They accessed the information with ease through an old security hole in the Zimbra VMWare service that army security technicians had omitted to patch.

Public administrations around the world, and in particular defense and national security services, are well aware of the risks they face. In 2016, **the US Department of Defense presented a pilot bounty program called "Hack the Pentagon," where rewards are offered to encourage hackers to find security flaws in the Pentagon's website, applications and networks.**

Russian hackers compromised the Pentagon's unclassified email system.

Latin American attackers compromised the email servers of the Bolivian army.

Despite the investment in cyber-security made by the U.S. government, one of the most recent attacks to come to light is the one that targeted the Democratic National Committee, which has acknowledged that its systems were compromised for at least a year. Evidence has been found to suggest that the attackers belong to Russian intelligence services, and that they have had access to emails, chats and a variety of research documents. All the computers in the committee's research department had been accessed and some files stolen.

In a similar vein, this July, a total of 19,252 emails and 8,034 attachments from the US Democratic National Committee sent between January 2015 and May 2016 were revealed on Wikileaks. The security company contracted by the Democratic National Committee has claimed that **the hack was the work of at least two different groups of hackers linked to a Russian government agency in an action designed to favor Republican candidate Donald Trump.**

Now, three months before the US elections, the FBI has confirmed the hacking of at least two electoral databases by foreign hackers who have extracted voter information from at least one of them. There is an ongoing investigation and IPs have been traced back once again to Russian hacking forums. Coincidence?

To prevent new attacks on public agencies, a common regulatory and legislative framework is needed, with responsibilities shared between states, bilaterally or through supranational institutions.

A year without protection

Democratic National Committee systems were compromised for at least a year.

19,252 emails with 8,034 attachments

from the US Democratic National Committee were revealed.

Two electoral databases were hacked

by foreign hackers who have extracted voter information.

Legislative Changes

Changes to the regulatory framework implemented by the Cybersecurity Act of 2015 were the result of the administration's need for effective resources and sufficient capacity to respond to the continuing (and constantly increasing) incidents caused by cyber attacks. There was also a shortage of information sharing, which was not being addressed by either public or private sector training.

Other factors that have led to this change in the security framework include the fact that, as illustrated above, the security of a nation is no longer limited to the defense of its borders and sovereignty, but also to ensuring the welfare of its society in the face of new risks.

One of the aims of the Cybersecurity Act of 2015 is to bring private industry and domestic nonfederal entities into a federal initiative directed at sharing information on cyber-threat indicators detected, and defensive measures taken to protect information systems and information accessible through or controlled by information systems.

Technology and Legislation

The emergence of new players from different backgrounds and with varying motivations combined with their ability to act in any security dimension, hinders the identification of aggressors and decreases the ability of countries to adequately respond. Current legislation is not adapted to the new cyber crime dynamic or to new technological or data management demands.

The Cybersecurity Act provides a paradigm for the sharing of information on cybersecurity threats and defensive measures among private sector entities and between the private sector and the government. It also provides liability protection to private sector entities for sharing cybersecurity threat information and defensive measures with the government and other private sector entities. Finally, it provides antitrust protection when information is shared only between private entities.

The liability protections included in the Cybersecurity Act largely mirror the language in both CISA and the House Intelligence Committee bill, with some slight variations. Private sector entities are required to remove personal information unrelated to a cybersecurity threat prior to sharing it through the Department of Homeland Security portal. DHS is also required to do a second scrub to remove personal information.

The key is that the Act requires the sharing of information in real time vs. other language discussed during Congressional deliberations that might slow the sharing process down and allow the intruder to disappear before countermeasures can be implemented.

Cybersecurity experts are now warning governments and citizens of the importance of protecting Internet systems and implementing tighter security than ever before, as, if action is not taken, the future consequences could be dire.

The solution for adapting to the change

Administrations are now promoting a shift away from a cyber-security model focused on protecting information (Information Security), towards a comprehensive security model based on the management of cyberspace risks (Information Assurance).

For public institutions, success in ensuring cyber-security lies with meeting certain requirements:

Real-time information

Having real-time information about incidents and security holes related to data security, such as the accidental or illegal destruction, loss, alteration, unauthorized disclosure or remote transference of data.

Foreign Report

Reporting all possible transfers of data files to foreign countries.

Privacy

Improving individual rights, including the right to be forgotten, and data portability across all shared data files.

Safeguard

Safeguarding delegation to other processors of data deletion, reporting and notification requirements, and the maintenance of file transfer activities.

Adaptive Defense 360

To this effect, the implementation of advanced technologies such as Adaptive Defense, as a complement to traditional antivirus solutions or perimeter security, enables compliance with the ENS and the technical requirements outlined above, since **Adaptive Defense offers guaranteed security against threats and advanced targeted attacks on companies via four basic pillars:**

Visibility:
Traceability and visibility of every action taken by running applications.

Detection:
Constant monitoring of all running processes and real-time blocking of targeted and zero-day attacks, and other advanced threats designed to slip past traditional antivirus solutions.

Response:
Providing forensic information for in-depth analysis of every attempted attack as well as remediation tools.

Prevention:
Preventing future attacks by blocking programs that do not behave as goodware and using advanced anti-exploit technologies.

Adaptive Defense protects computers by only allowing legitimate software to run, while monitoring and classifying all processes running on a customer's infrastructure based on their behavior and characteristics. It also provides monitoring tools, forensic analysis and incident resolution to determine the extent of any problems detected and how to resolve them.

Unlike traditional antivirus software, Adaptive Defense leverages a new security model that allows it to adapt precisely to the specific environment of each company, monitoring the execution of all applications and constantly learning from the actions triggered by each process.

After a brief learning period, **Adaptive Defense 360 is able to offer levels of protection way above those of traditional antivirus products,** as well as providing valuable information regarding the context in which security problems occur, in order to determine their scope and implement preventative measures.

Adaptive Defense is a **multi-platform service that supports Windows, Linux, Mac OS X, and Android.** As it is hosted in the cloud, there is no need for investment in additional IT infrastructure, ensuring a low TCO.

As a cloud-based managed security service, the National Security Framework (ENS) requirements are the direct responsibility of the service provider. **Panda Adaptive Defense is hosted on Microsoft's Azure cloud.**

Microsoft Azure has undergone rigorous testing by BDO, an independent auditor, who has officially certified compliance. BDO certifies that the security measures of the service, as well as those of the IT Systems and installations for processing data, offer high level compliance with RD 3/2010, with no need for remedial measures.

Finally, it is important to underline that **Adaptive Defense does not gather any personal data and under no circumstances does it send personal data to the cloud,** thereby ensuring compliance with current and future data protection legislation.

Protection against advanced threats and targeted attacks, with the ability to detect anomalous behavior. A system for ensuring data confidentiality, information privacy and safeguarding an organization's assets and reputation. All that is Adaptive Defense, the only advanced cyber-security system that combines next generation protection with the latest detection and remediation technologies able to classify all running processes.

More information at:

BENELUX
+32 15 45 12 80
belgium@pandasecurity.com

BRAZIL
+55 11 3054-1722
brazil@pandasecurity.com

FRANCE
+33 (0) 1 46842 000
commercial@fr.pandasecurity.com

GERMANY (& AUSTRIA)
+49 (0) 2065 961-0
sales@de.pandasecurity.com

HUNGARY
+36 1 224 03 16
hungary@pandasecurity.com

ITALY
+39 02 24 20 22 08
italy@pandasecurity.com

MEXICO
+52 55 8000 2381
mexico@pandasecurity.com

NORWAY
+47 93 409 300
norway@pandasecurity.com

PORTUGAL
+351 210 414 400
geral@pt.pandasecurity.com

SOUTH AFRICA
+27 21 683 3899
sales@za.pandasecurity.com

SPAIN
+34 900 90 70 80
comercialpanda@pandasecurity.com

SWEDEN (FINLAND & DENMARK)
+46 0850 553 200
sweden@pandasecurity.com

SWITZERLAND
+41 22 994 89 40
info@ch.pandasecurity.com

UNITED KINGDOM
+44(0) 800 368 9158
sales@uk.pandasecurity.com

USA (& CANADA)
+1 877 263 3881
sales@us.pandasecurity.com

More information at:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

by calling:

+1 877 263 3881

or by email sales@us.pandasecurity.com

panda

Adaptive Defense 360

Limitless Visibility, Absolute Control

pandasecurity.com

panda