Threat Intelligence

Building Trust for Better Citizen Engagement

Trusted partner for your **Digital Journey**

Atos

Introduction

City and state government planners are increasingly engaging citizens through mobile applications and other digital services, enabling them to pay bills online, communicate with city officials on social media, schedule the use of a public facility, and travel more efficiently through cities via intelligent transportation systems.

The growth of digitally-connected citizens and ongoing digitization of governments and society increases the need for more real-time data for city officials and citizens to make more informed decisions. Additionally, the gathering and analysis of massive amounts of data requires a vast array of IT systems, operational technology, and Internet of Things (IoT) sensors and devices that must be secure to protect government data and citizens' private information.

For smart cities to be truly smart, city planners and IT cyber teams must incorporate threat intelligence and a solid cyber security posture that both mitigates risk and, at the same time, enables citizen engagement. Delivering an effective citizen experience requires a holistic approach using data to capture and understand their needs and desires.

Accurate and timely communication is the foundation for government engaging successfully with citizens. Although the tools and methods to actively engage communities have undergone a significant evolution over the past few years, ensuring data security and privacy must remain a top priority despite the rapid developments in technology.

New York City Mayor Bill de Blasio acknowledged the role of government in protecting citizens online in March 2018 during the launch of NYC Secure, a pioneering cyber security initiative aimed at protecting New Yorkers online. The first NYC Secure programs will include a free city-sponsored smartphone protection app that, when installed, will issue warnings to users when suspicious activity is detected on their mobile devices. The city additionally announced new world-class protection for its public Wi-Fi networks, becoming the first city in the world to provide such services to all residents and visitors free of charge.

"New Yorkers manage so much of their lives online, from paying bills to applying for jobs to engaging with government. NYC Secure will ensure that we're applying the best and most effective protection efforts to help New Yorkers defend themselves online," de Blasio said. Geoff Brown, citywide chief information security officer and head of NYC Cyber Command, also said, "In order to stay a step ahead of cyber criminals that are continuously finding new ways to hack devices, we must invest in the safety of the digital lives of our residents."

Protecting citizens' data and privacy in a digital-connected world is a complex and daunting task. City planners should first identify applications where they can engage the public, such as street lighting, traffic lights, and parking meters. "These are usually the low-hanging fruit to get the ball rolling," said Robert Masterson, a security consultant with Atos, a leader in digital services, providing consulting and system integration services as well as big data and cyber security solutions.

Often, city planners and citizens do not think enough about the risks associated with new technology. People do not know if the banking application on their smartphone is secure or understand the consequences of using the same phone for social media, chat and other apps simultaneously, said David Storch, also a security consultant with Atos.

City planners "will look at a new mobile app with a lot of enthusiasm, but not bring the same level of rigor to examine the security ramifications" of new technology, Storch said. But city planners in state and local government must recognize that they are not responsible for just protecting government assets and data. They are equally responsible for making sure citizens' data and privacy are protected — citizens that are entrusting confidential information to government agencies.

Improving the citizen experience

Delivering an effective citizen experience requires a holistic approach to the citizen, which includes:

1. Using data to capture and understand the needs and desires of the citizen;
2. Leveraging effective social media and communications to actively engage citizens;
3. Allowing the citizen to engage on his or her own terms;
4. Understanding the citizen's preferred engagement channels;
5. Affording seamless transitions among channels;
6. Ultimately delivering a more satisfying set of citizen interactions.

Adopting a citizen-centric information management strategy with multichannel citizen engagement opportunities will deliver quantifiable benefits.

Risk assessment: vital first step

To protect the digital lives of residents, city and state government leaders need to conduct a "bona fide risk assessment" of all digital services and their connections, the vast array of IT systems, operational technology, IoT sensors, and mobile devices that make up a city's digital ecosystem.

City planners must bring in security professionals to do a proper risk assessment. Some applications will have more risk than others, and the applications that provide the least risk are the ones that city officials should open to the public first, Storch advised.

To help governments implement a proper risk assessment of their IT, the National Institute of Standards and Technology (NIST) set forth a Risk Management Framework (RMF), which details a set of criteria that dictates how federal government IT systems must be architected, secured, and monitored.

The RMF defines a six-step process to architect and engineer a data security process for new IT systems and suggests best practices and procedures federal agencies can implement to secure systems. These best practices and procedures can be applied just as well by state and local governments with the help of security professionals. [1]

For example, the first step: Categorize the System will help city planners determine viable threats to the system, process, functions, or application. This would be achieved by focusing on factors such as: What is the system? What kind of data does it use? Who is the vendor? What internal and external interfaces does the system use? Who uses the system? What is the data flow and where does the information go?

In May 2018, NIST released an RMF update, formally titled Draft NIST Special Publication (SP) 800-37 Revision 2. Previous versions of the RMF were primarily concerned with cyber security protections from external threats. The updated version adds an overarching concern for individuals' privacy, helping to ensure that organizations can better identify and respond to these risks, including those associated with using individuals' personally identifiable information, according to NIST.

The update is also interesting because it connects the RMF with NIST's well-known Cybersecurity Framework (CSF), highlighting relationships that exist between the two documents. The CSF, which was released in 2014, consists of standards, guidelines, and best practices for the protection of critical infrastructure and for improvements to government security. The Framework offers five core functions that act as a backbone for a holistic approach to information security: identify, protect, detect, respond, and recover. Companies are using these concepts to align their security tools with CSF's guidance on implementing security controls and measures.

In April 2018, a new version of the CSF was released to include guidance on how to perform self-assessments, additional details on supply chain risk management, and guidance on how to interact with supply chain stakeholders.

State government agencies are using the Framework to protect information and information technology assets. For instance, the Framework is helping the Multi-State Information Sharing & Analysis Center (MS-ISAC) enable agencies to develop a benchmark to gauge year-to-year progress across the Framework's functions and categories. It also provides organizations with metrics to see how they rate compared to similar organizations.

[1] The six RMF steps include: Categorize the information system and the information processed, Select an initial set of baseline security controls, Implement the security controls, Assess the security controls, Authorize the information system's operation, and Monitor the security controls in the information system on an ongoing basis.

Both the CSF and the RMF frameworks serve as a guide for governments that are looking to improve their cyber security and risk mitigation practices. It is vital, now more than ever, for state and local officials to utilize these frameworks in an increasingly digital world.

Six steps to better risk management (RMF)

The Risk Management Framework, maintained by The National Institute of Standards and Technology, is a set of criteria that dictate how federal government IT systems must be architected, secured, and monitored. RMF includes a six-step process.

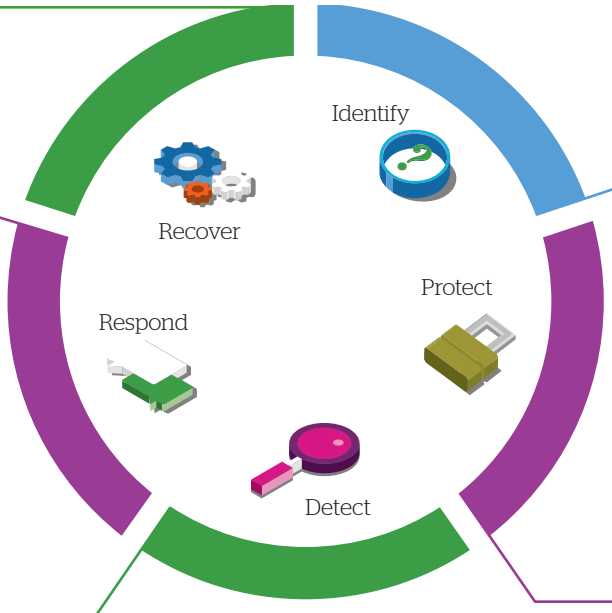
1. **Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
2. **Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
3. **Implement** the security controls and describe how the controls are employed within the information system and its environment of operation.
4. **Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
5. **Authorize** the information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
6. **Monitor** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational official.

Source: NIST

The five security framework functions

Recover
The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Respond
The Respond Function includes appropriate activities to act regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.



Identify
The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Protect
The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

Detect
The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.

Source: NIST

Threat intelligence: a tool for secure citizen engagement

What is threat intelligence? And why is it an important tool for state and local government leaders to securely engage with citizens? The term 'threat intelligence' is often used loosely. As defined by Gartner, threat intelligence is "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

Currently, threat intelligence takes many forms. Sometimes it is provided via dedicated feeds. For instance, based on activity from millions of sensors worldwide and an extensive research team, a global threat information company can publish timely, relevant threat activity to subscribers.

Increasingly, threat intelligence capabilities are built into common security products such as firewalls, IPS, and gateways to reduce operational efforts and time between detection and containment. Standard devices are increasingly leveraging threat information and reputation feeds to improve their overall security performance.

"Threat Intelligence is the ability to recognize. Intelligence boils down to, 'Did you recognize what was going on in many cases?'" Masterson noted. "You can't solve a problem that you don't know is there. There is a correlation between recognition of an issue and the resolution of an issue," he said.

Moreover, this intelligence helps state agencies prioritize actions in proportion to the threat. Organizations have attempted to introduce threat intelligence into their security tooling in order to detect and protect against known malicious domains, blacklisted Internet addresses and other identifiers. But this intelligence can sometimes consist of millions of indicators that overwhelms security personnel.

Sheer volume of data is not necessarily good; data must be processed and analyzed to make it useful.

Citizen engagement: providing a secure foundation

The unfolding, digitally-connected world provides government leaders the opportunity to engage and work in real partnership with citizens. In fact, there is real opportunity for citizens to co-design and co-implement programs in partnership with government.

A secure, digital foundation, which protects citizens' data and privacy, can help government organizations move beyond traditional models of governance where citizen input is received once per election cycle or not at all, to one that is more open, inclusive and responsive to citizens. This model of governance would ensure that citizen input is sought on a regular basis, including from the most marginalized groups.

The rise in social media platforms now means that citizens increasingly demand that their individual voices be heard. They prefer viewing and sharing information about their communities and issues that affect them and participating online in active discussions versus passively absorbing messages from their government. "By engaging citizens, government agencies can improve the delivery and quality of public services, enhance the management of public finances, and bring about greater transparency, accountability and social inclusion, resulting in tangible improvements in people's lives," Soren Gigler, who lead the Mapping for Results Initiative at the World Bank Institute, wrote in a 2016 World Economic Forum blog.

Moreover, "citizen engagement signifies a cultural change in the way government approaches development, whereby local communities drive the process of development that shapes their lives," Sigler wrote. "The most sustainable results are achieved when citizens become active agents rather than passive recipients."

To make citizen engagement meaningful, governments and citizen groups need to work together to develop institutionalized methods of receiving and responding to citizen input.

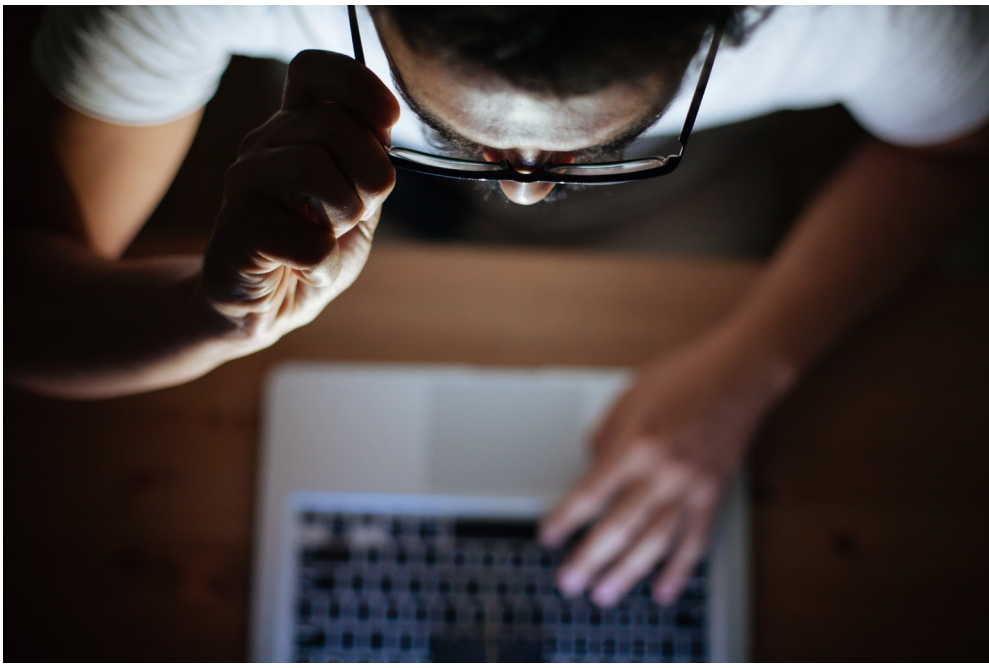
To make this possible, government leaders and city planners must adopt a proactive and intelligence-based approach to cybersecurity that can detect cyber threats before they can do harm to government assets and citizens' data and privacy.

Three levels of threat intelligence

Industry analysts have identified three key levels of cyber threat intelligence:

- **Tactical:** Technical intelligence such as using threat indicators to proactively hunt for and defend against adversaries.
- **Operational:** Intelligence focused on the motivations, intent and capabilities of adversaries.
- **Strategic:** Intelligence about the risks and implications associated with threats used to inform business decisions and direct cyber security investment.

Identifying threats means that agencies can combine different levels and types of intelligence (including human intelligence) to obtain targeted, contextual threat intelligence in relation to their brand, their people and their technology. This proactive and structured approach adds immense value by enabling greater insight into what threats the agency faces, the tactics, techniques, and procedures of its adversaries, and how this can be used to minimize disruption of business or an agency's mission and reduce the window of opportunity for attackers.



Atos vision for cyber security and threat mitigation

Learning the lessons of the past is now vital, as is embracing technological innovation. In response, governments are starting to make the move to prescriptive security, which is security that leverages big data, super computing capabilities and machine learning to specify both the actions necessary to achieve predicted outcomes, and the interrelated effects of each decision. This technology, combined with human insight, allows organizations to identify anomalies very quickly to predict – and even prevent – attacks.

Atos Prescriptive Security, an integrated service, is helping organizations stay ahead of the growing complexity and volume of threats by continually learning and orchestrating automated security actions to resolve current threats and anticipate new ones.

Going forward, governments will have to focus on making cyber security a board-level issue, applying enterprise-wide risk management, accessing leading-edge security solutions, and effectively engaging and educating employees to keep their organizations and their stakeholders safe in an increasingly unpredictable world.

Vital steps to take when combating threats

As governments build their arsenal against cyber threats, here are four vital steps that should be taken:

Define the risks and governance: Build a tailored and resilient cyber security strategy. City planners and IT cyber teams should understand the landscape they are working in. What would happen if your organization came under attack and how would you minimize the disruption to critical services? Breaches are inevitable so make sure you have contingency plans in place.

Threat intelligence: Build a threat hunting program. Threat hunting is fundamental since it can identify and eliminate vulnerabilities before threat actors discover them. To build such a program, agency managers will need a cyber threat intelligence service that could aggregate intelligence gathered from security testing, from manufacturers, and threat information service providers. Aggregating and transforming such intelligence into actionable insight is essential as the threat landscape continues to change at a fast pace.

Cyber deception: Take a preemptive approach and understand potential attackers' activities and techniques. This requires creating virtual twin environments to lure attackers into 'honey pots' and study what they're doing. This way you can contain them from critical environments and take immediate action to neutralize the cyber attacks.

Adaptive security: This approach to security incorporates analytics and automation. The sheer scale of IoT, cloud and citizen data is simply overwhelming; accordingly, AI will be the biggest tool in the cyber security arsenal in the years to come. It will be able to detect and respond in real-time, self-learn proactively from the internal and external environment and automatically make alterations to block attacks.

Agencies should evaluate several areas of threat intelligence, including:

- Broad-based vulnerability management to not only discover vulnerabilities across the landscape (including IoT and the cloud) but to prioritize these threats according to the risks they pose to citizen data.
- Continuous dark web scanning, either by the agency themselves or by subscribing to threat feeds and/or multi-state information sharing programs.
- Creation of data lakes — which will be required to scale with the amount of threat data from IoT, OT, cloud and citizen engagement services.
- Increasing use of analytics to create risk-based approaches to threat management. An increasing number of vendors are bringing risk-based analytics to the market to help score users, applications and machines so that agencies know how to prioritize security activities.

Security is strengthened as more and more data is gathered and analyzed, and by pooling together information from multiple agencies, cities and states. Another option for agencies would be to subscribe to — or outsource — security services to global MSSP's such as Atos.

The bottom line

The rise of innovative technology and social media platforms has increased citizen expectations when it comes to interacting with government and has provided citizens with opportunities to have a greater say in decision-making and directly engage with elected officials and policy makers – paving the way for true partnership between citizens and governments.

As a result, state and local government officials will need an automated, intelligence-based approach to cyber security that can protect government assets as well as ensure the data integrity and privacy of their citizens in an increasingly digitized world. Governments will need to make use of cloud platforms to be more flexible and to improve operational efficiencies. Additionally, governments are increasingly turning to a wide variety of IoT devices — such as smart meters and smart traffic systems — to improve services and reduce costs. These initiatives have clear benefits, but to deliver those benefits securely, appropriate risk management processes must be put in place.

Moreover, state and local government leaders will need to break apart the silos that keep agencies from communicating and sharing security information. For instance, The Department of Motor Vehicles and Department of Children's Welfare should not conduct security in their own way, with their own threat feeds, and without the departments communicating with one another. Threat feeds get better by gathering more information. There must be common backbones and information sharing as close to real-time as possible and agencies should make use of automation as much as they can.

"There will always be a need for human evaluation," Storch said. However, the machines should be learning and observing system and network behavior as well as sifting through data. Security professionals can then look at the outputs and do analysis, Storch said.

With the right threat intelligence and cyber security measures in place, governments have the opportunity to better engage their citizens, build trust, and keep the public's data safe as technology evolves. For more information on how Atos can help state and local governments on the path to threat intelligence and better citizen engagement, visit here.

About Atos

Atos is a global leader in digital transformation with 120,000 employees in 73 countries and annual revenue of € 13 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions through its Digital Transformation Factory, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies and industry knowledge, Atos supports the digital transformation of its clients across all business sectors. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Syntel, Unify and Worldline. Atos is listed on the CAC40 Paris stock index.

Find out more about us

atos.net

Let's start a discussion together

To learn more about Atos' security solutions:
https://atos.net/en/solutions/cyber-security