UNCLASSIFIED / NON CLASSIFIÉ

Citizen FIRST | POWERED BY Institute for Citizen-Centred Service

Building a Cybersecurity-aware Culture in Public Sector Organizations

- Importance of a Proper Cybersecurity-aware Culture in Public Sector Organizations
- Foundations of Cybersecurity Culture in Public Sector
- Strategies for Implementation
- Measurable Objectives and Action Plans
- Challenges, Risks, Opportunities

JOINT COUNCILS' EXECUTIVE MONTHLY REPORT

Developed by the Research Committee

September 2023

Images: iStock

1. Importance of a Proper Cybersecurity-aware Culture in Public Sector Organizations

In the era of digital transformation increasingly reliant on digital platforms, public sector organizations should always aim to fortify their cyber defenses. As a result, since protecting critical information assets is paramount, a cybersecurity-aware culture ensures that all employees act as a strong defense line.

Cybersecurity is not a destination but a continuous journey. Government agencies must keep evolving their strategies to stay ahead of emerging threats. A culture of awareness enables agility and responsiveness in adapting to the dynamic cybersecurity landscape.

A comprehensive understanding of cybersecurity across all levels creates a unified approach to risk management. This organizational awareness is not just about technology but encompasses policies, procedures, and people. A cybersecurity-aware culture minimizes the likelihood of successful cyber-attacks.

Collaboration within and across government agencies is essential for an effective cybersecurity strategy. A shared culture fosters communication, cooperation, and collective problem-solving. It builds a unified front against the multifaceted threats that cyber criminals present.

Citizens trust public sector organizations with their personal and sensitive information. Breaches can erode this trust and have lasting impacts on the public's perception. Cultivating a cybersecurity-aware culture helps preserve the integrity of the systems and maintains citizens' confidence.

Sources: Al Hogail, Areej. "Cultivating and assessing an organizational information security culture; an empirical study." International Journal of Security and Its Applications 9, no. 7 (2015): 163-178;
Gcaza, Noluxolo, Rossouw von Solms, and Joey Jansen van Vuuren. "An Ontology for a National Cyber-Security Culture Environment." In HAISA, pp. 1-10. 2015.

Why Is This Report Important?

The adoption of a cybersecurity-aware culture in public sector organizations is a strategic necessity in the current digital age. Cyber threats are evolving, and traditional security measures alone are insufficient. Understanding the criticality of a security culture can drive the implementation of robust practices that align with national interests.

Collaboration, awareness, and shared responsibility are vital for a strong cybersecurity framework. This report sheds light on the mechanisms to foster this environment. The insights provided are designed to guide policymakers in creating laws, regulations, and incentives that support a comprehensive cybersecurity approach.

A coherent, government-wide approach to cybersecurity is integral to protecting national interests. This report contributes to that goal by highlighting the essential components of a cybersecurity-aware culture. It serves as a roadmap for public sector organizations to align their cybersecurity practices with broader governmental objectives.

What is Covered in this Executive Report?

This report includes the following:

- Importance of a Proper Cybersecurity-aware Culture in Public Sector Organizations
- Foundations of Cybersecurity Culture in Public Sector
- Strategies for Implementation
- Measurable Objectives and Action Plans
- Challenges, Risks, Opportunities

2. Foundations of Cybersecurity Culture in Public Sector

The establishment of a cyber-secure culture within government organizations is a multidimensional effort that transcends technology. Let’s explore the key foundational pillars that contribute to shaping such a culture.

Shared Responsibility Across Departments: Cybersecurity is not confined to the IT department; rather, it is a collective endeavor. Each department and agency must be cognizant of its role in protecting their digital assets and public data.

Holistic Education and Training: Ongoing training and educational initiatives are central to ensuring that staff at all levels have the competencies needed to identify and mitigate cybersecurity threats. The curriculum should be adaptive and cater to the varying roles within the organization.

Leadership Commitment: The cornerstone of a cyber-secure culture is the unequivocal commitment from leadership. Their active engagement in cybersecurity initiatives not only sets the organizational tone but also ensures resource allocation and policy enforcement.

Robust Policies and Standard Operating Procedures (SOPs): Clearly articulated and widely disseminated policies provide a structural framework for cyber-secure behaviors. These should be accessible, easy to understand, and regularly updated to adapt to the evolving threat landscape.

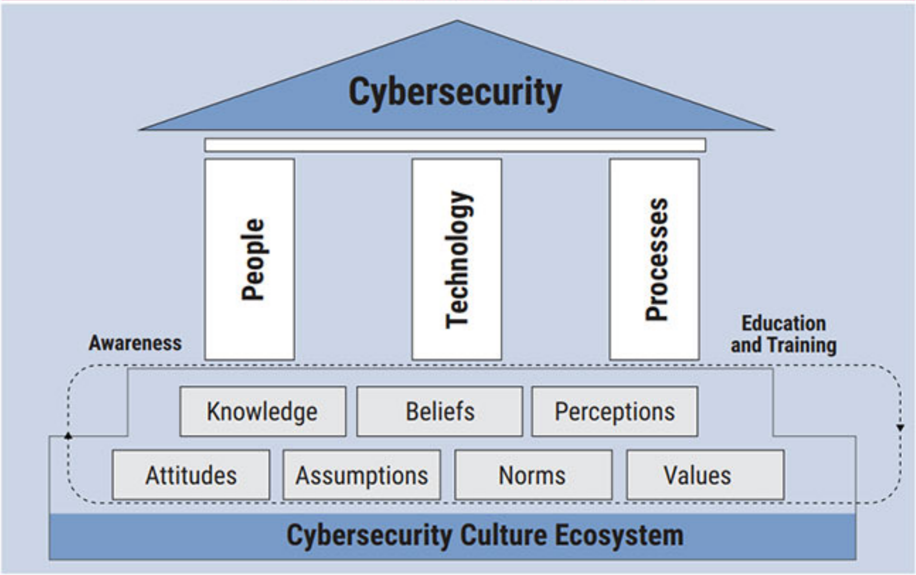
Human-Centric Technology Solutions: While technology is an indispensable tool, its efficacy is maximized when tailored to the human elements of the organization. The goal is to integrate technology solutions that are intuitive, user-friendly, and aligned with day-to-day operations.

Accountability and Transparency: Earning and maintaining public trust is crucial. This can be achieved through transparent practices and by holding all members accountable for their actions related to cybersecurity.

Inter-Agency Cooperation: Collaboration among various governmental bodies amplifies the effectiveness of cybersecurity measures. A unified strategy, built on shared resources and intelligence, enhances the government's collective ability to thwart cyber-attacks.

Consider the cybersecurity culture ecosystem framework suggested by the Information Systems Audit and Control Association (ISACA) below.

Figure 3—Centrifugal Culture Ecosystems Drivers



Sources: Möller, Dietmar PF. Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. Vol. 103. Springer Nature, 2023.; ISCACA: Implementing a Cybersecurity Culture (2019); Uchendu, Betsy, Jason RC Nurse, Maria Bada, and Steven Furnell. "Developing a cyber security culture: Current practices and future needs." Computers & Security 109 (2021): 102387.

3. Strategies for Implementing Cybersecurity-aware Culture

Implementing a cybersecurity-aware culture in public sector organizations requires a structured and strategic approach. Leveraging best practices, tailoring training, and building cross-sector collaboration are fundamental to this transformation.

Building Awareness and Education

- Cybersecurity awareness must begin at the top. Leadership must be well-informed and committed to championing the cause, aligning it with organizational goals, and providing the resources necessary for effective training and education.

- Tailoring cybersecurity education to different roles within the organization is essential. From frontline staff to IT professionals, each individual must understand their specific responsibilities and the implications of their actions on overall cybersecurity.

Technology and Infrastructure

- Implementing technology solutions that align with the organization's cybersecurity goals is paramount. This involves not just deploying cutting-edge tools but also ensuring that they are configured correctly, maintained regularly, and integrated seamlessly within existing infrastructure.

- Cybersecurity isn't just about defending against external threats. Internal controls and monitoring systems are equally critical. Implementing robust authentication procedures, regular security audits, and incident response plans helps in maintaining a secure environment.

Policy and Governance

-Clear and enforceable policies and procedures form the backbone of a cybersecurity culture. These policies should be regularly updated to reflect changing threat landscapes and regulatory requirements and must be communicated effectively to all staff.

- Governance structures that facilitate cross-departmental collaboration and ensure accountability at all levels are crucial. A dedicated cybersecurity governance body can oversee the implementation, monitoring, and continuous improvement of cybersecurity practices across the organization.

Collaboration and Information Sharing

- Collaborative platforms that allow public sector organizations to share threat intelligence, best practices, and resources enhance the collective defense against cyber adversaries.

- Trust is essential for effective collaboration. Building formal agreements, ensuring confidentiality, and creating secure channels for communication encourages organizations to share valuable information without fear of compromising sensitive data.

Sources: Georgiadou, Anna, Spiros Mouzakitis, and Dimitris Askounis. "Detecting insider threat via a cyber-security culture framework." Journal of Computer Information Systems 62, no. 4 (2022): 706-716.

4. Measurable Objectives and Action Plans

Measurable objectives and action plans provide the blueprint for implementing a cybersecurity-aware culture. Establishing clear targets and actionable steps, supported by regular monitoring and review, ensures that the strategy is effectively translated into practice.

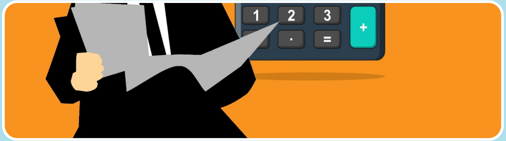
Define clear, specific, and measurable cybersecurity objectives that align with organizational goals. These objectives must reflect both short-term and long-term targets. They should be communicated across the organization and be linked to individual performance metrics. Regular assessments ensure that progress is tracked and adjustments are made as needed.

Create actionable plans that outline the steps to achieve each objective. These plans must include timelines, responsible parties, and required resources. Actionable plans foster accountability and ensure that everyone knows their role in achieving cybersecurity goals. Collaborative planning, involving different departments, enhances the comprehensiveness and effectiveness of these plans.

Implement monitoring mechanisms to regularly assess the progress of the action plans. Regular monitoring provides insights into what is working and what needs improvement. It enables timely interventions and ensures that the plans remain aligned with the changing cybersecurity landscape. Feedback loops involving all stakeholders enrich the monitoring process and foster continuous improvement.

Foster a culture of continuous improvement and learning. Cybersecurity is a dynamic field, and a static approach can quickly become outdated. Encouraging a culture that embraces change, learns from successes and failures, and constantly seeks improvement keeps the organization agile and responsive to emerging threats.

Collaboration across different government entities is vital in achieving a unified cybersecurity approach. Shared objectives and coordinated action plans enable a synergistic approach to cybersecurity. Regular inter-agency meetings, aligned reporting mechanisms, and collaborative projects enhance the collective ability to respond to cyber threats. This collaboration extends beyond government, involving the private sector and international partners, where applicable.

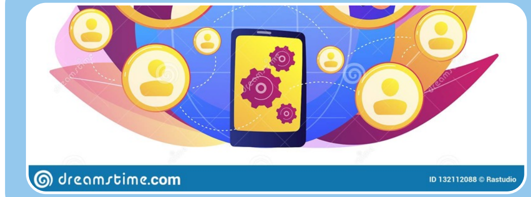


Encourage innovation and research within the public sector to keep abreast of the latest cybersecurity trends and solutions. Investment in research and development ensures that the public sector stays ahead of the curve in cybersecurity. Fostering partnerships with academia, private sector, and other research institutions promotes innovation. Regularly updating strategies based on research findings ensures that the public sector remains an active player in shaping the future of cybersecurity.

Sources: Trim, P. and Upton, D., 2016. Cyber security culture: Counteracting cyber threats through organizational learning and training. Routledge; Gcaza, Noluxolo, Rossouw von Solms, and Joey Jansen van Vuuren. "An Ontology for a National Cyber-Security Culture Environment." In HAISA, pp. 1-10. 2015; Ghernaouti, Solange, and Bastien Wanner. "Research and education as key success factors for developing a cybersecurity culture." Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden (2018): 539-552.

5. Challenges, Risks, and Opportunities

Recognize and address the diverse challenges that come with building a cybersecurity-aware culture. These challenges may include resistance to change, limited resources, and the complexity of integrating various cybersecurity components. Open dialogue, dedicated resources, and strong leadership commitment can mitigate these challenges and facilitate a smooth transition.



Identify and mitigate the risks associated with the cybersecurity transformation. Risks may include potential security gaps during the transition, potential conflicts with existing regulations, and unforeseen consequences on other organizational functions. A robust risk management framework that includes regular risk assessments, mitigation strategies, and monitoring mechanisms can manage these risks effectively.

Embrace the opportunities that a cybersecurity-aware culture brings to public sector organizations. These opportunities may include enhanced collaboration, improved public trust, and increased resilience against cyber threats. Capitalizing on these opportunities requires a proactive approach, continuous improvement, and alignment with broader governmental strategies.

Acknowledge the role of external stakeholders in shaping the cybersecurity landscape. Partnerships with private sector, international bodies, and other governmental entities provide opportunities for shared learning and collaboration. These relationships must be nurtured and managed effectively to leverage the unique strengths and perspectives that each party brings.

Cultivate a mindset that views cybersecurity as an enabler rather than a barrier. Changing the perception of cybersecurity from a hindrance to an enabler of organizational goals fosters acceptance and integration into daily operations. This mindset shift encourages innovation, enhances collaboration, and creates a more resilient and agile organization.

Sources: Corradini, Isabella. Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology. Vol. 284. Springer Nature, 2020.

For Further Reading

- Nagyfejeo, Eva, and Basie Von Solms. "Why do national cybersecurity awareness programmes often fail." International Journal of Information Security and Cybercrime 9, no. 2 (2020): 18-27.
- Christine, Debora, and Mamello Thinyane. "Cyber Resilience in Asia-Pacific: A Review of National Cybersecurity Strategies." (2020).
- Teoh, Chooi Shi, and Ahmad Kamil Mahmood. "Cybersecurity workforce development for digital economy." The Educational Review, USA 2, no. 1 (2018): 136-146.
- Nurse, Jason. "A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK." (2017).
- Murray, Peter J., and Roger J. Ward. "Promoting enterprise risk management (ERM) and governance, risk and compliance (GRC) for managing cybersecurity risks." (2018).
- Saputra, Pradipta Nindyan, Arfin Sudirman, Obsatar Sinaga, Wahyu Wardhana, and Nurul Hayana. "Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP)." Central European Journal of International & Security Studies 13, no. 4 (2019).

Other noteworthy articles:

- Hoggard, Amy. "Comparing Canadian and American cybersecurity awareness levels: Educational strategies to increase public awareness." PhD diss., Utica College, 2014.
- Mishra, Alok, Yehia Ibrahim Alzoubi, Memoona Javeria Anwar, and Asif Qumer Gill. "Attributes impacting cybersecurity policy development: An evidence from seven nations." Computers & Security 120 (2022): 102820.

Research Repository

Access the Citizen First Research Repository.

Recent entries on the research repository:

Defining Bias in AI and Government Service Delivery

This report includes the following:

- Importance of Defining Bias In AI and Government Service Delivery
- Identifying Types and Sources of Bias in AI
- The Intersection of Bias and Ethics in AI in Gov-t
- Strategies and Measures to Mitigate Bias

Trends in the Daily Newsletter

Service Canada has been working diligently to deliver high-quality, simple, easy-to-access and secure services to Canadians, no matter where they live. As technology advances and clients' service delivery expectations change, the Government of Canada is taking steps to further modernize its delivery methods and available services.

As part of these modernization efforts, Service Canada has improved the online My Service Canada Account (MSCA) to allow anyone with an account to view their Social Insurance Number (SIN) securely online.

Terry Beech, the first-ever federal minister of citizens' services, recently told CBC News that one of the priorities in his new role will be to make federal government services "digital first" and "digital by design."

He also shared that he's open to using new technologies like AI to help improve how the government delivers services to Canadians.

"I'm sure there will be some people that get concerned when we talk about digital first," Beech noted. "Digital first does not mean that we won't have in-person options or options over the telephone."

Canada became the first country in the world to approve an AFC operator for commercial operation.

This means Canada will become the first country with commercially operating standard power 6 GHz Wi-Fi services within an estimated couple of months.

The designation was announced by ISED – a Canadian government department – naming Qualcomm as the country's first 'Automated Frequency Coordination System Administrator' or AFCSA. It's also a world first for Qualcomm and for the Wi-Fi industry.

We would love to hear from you!

Do you know someone who may be interested in the Joint Councils Executive Report? Please share a copy of this report. If you are not already a subscriber, you can now subscribe to receive the Executive Report by signing up. Send your questions to info@iccs-isac.org.

Follow: