
accenturesecurity
ACCENTURE CYBERSECURITY FORUM
WOMEN'S COUNCIL
Privacy, security and digital inclusion: How to use today's technology for digital inclusion tomorrow
Virtual Roundtable Summary
December 18, 2018

DISCUSSION

On December 18, 2018, the Accenture Cybersecurity Forum Women's Council hosted a discussion on "Privacy, security and digital inclusion: How to use today's technology for digital inclusion tomorrow." Female CISOs and senior security executives from multiple organizations and industries joined the conversation with our guest subject-matter expert, a cybersecurity director.

The discussion highlighted the challenges facing CISOs and other leaders in improving digital inclusion and helping stakeholders maintain secure digital identities, and explored best practices for addressing these important issues. The session was held under the Chatham House Rule. Below is a high-level summary of the discussion without attribution. Council members may use the information provided that neither the identity of the speaker nor that of the speaker's organization is revealed.

The many dimensions of digital inclusion

Digital inclusion is a global challenge. The estimated 1.5 billion people living without an officially recognized digital identity may not be able to access financial and health care services and engage in a variety of other activities that many of us take for granted. Even for people who do have a recognized identity, it can be difficult to preserve privacy, authenticate identity and operate securely in a digital world. Enterprises across geographies and industries have learned that maintaining the privacy and security of their employees, partners and customers is a fundamental cost of doing business.

Several important trends are reshaping identity in the digital world:

- Expectations are increasing for human-centric and personalized experiences, as well as expectations that individuals should have the ability to control their own identities with high levels of security and privacy. There is potential for

establishing a single digital identity that can work throughout a person's life across a wide variety of interactions and transactions.

- Disruptive technology, particularly mobile devices, biometrics, AI and robots, can be part of the solution to increasing digital inclusion. However, there will be challenges in terms of adoption, interoperability and security.
- Blockchain technology—which features cryptographically secure data, makes tampering self-evident, and operates in a decentralized, distributed environment—potentially enables stakeholders to establish one identity across multiple entities. The promise of blockchain is to provide a framework of trust that changes how people work and share data. Pilot projects within the enterprise and across groups of organizations can be useful in creating value from blockchain technology.
- User centricity should be a core consideration in creating and deploying digital identities. Stakeholders need to understand the implications of sharing their personal information. Enterprises must develop user ID systems beyond today's user name and password solutions. Although the definition of a "good" digital identity has not been universally established, from a user-centric perspective a digital identity should be useful, inclusive, and secure; offer choice; and fit its purpose.
- A collaborative ecosystem (a "web of trust") may be required to achieve greater digital inclusion and identity interoperability. However, many issues—including security, privacy, legal, compliance, systems requirements, ethics, adoption and human centricity—will need to be addressed. Challenges of this scale can be solved only through joint public and private initiatives. It's challenging to get everyone together on the same page, and it's not an issue that can be solved company by company or even among groups of companies.
- Until a universal collaborative ecosystem is established, initiatives will emerge from a variety of business sectors. For example, the financial services industry is

a leader in secure digital identification. However, CISOs cautioned that financial institutions should not be expected to independently establish a one-size-fits-all digital identity model.

- Bad actors who threaten digital security and privacy are exponentially increasing their abilities and efforts, according to a senior law enforcement spokesperson. While law enforcement is effective in identifying the perpetrators of economic espionage, enterprises have a deeper understanding of the information bad actors are pursuing. Collaboration between these two parties will be essential to strengthening cybersecurity.

Key takeaways

- **Digital inclusion is becoming a high priority**—Despite challenges, CISOs have reason to be optimistic about improved digital inclusion. The issue is receiving significant attention from governments, non-governmental organizations (NGOs) and enterprises. Models of expanding digital inclusion differ among geographic regions, but the need is becoming a global priority.
- **Collaboration and partnership are essential to overcoming challenges**—All industries face similar challenges in enhancing digital inclusion while increasing privacy and security. Collaborative, cross-industry initiatives are essential to creating high-quality digital identities that work across multiple platforms. Governments, NGOs and tech companies will be crucial partners in these efforts.
- **Authentication is a rising concern**—In a digital world of the Internet of Things, the idea of "identity" will extend beyond people. Device authentication among a variety of assets, including natural resources, factory equipment, mobile devices, cryptocurrency and vehicles, will be required for digital transformations. CISOs should plan accordingly.

DISCUSSION

- **Emerging technology should be evaluated and adopted**—CISOs are encouraged to examine and pilot emerging technologies such as blockchain, biometrics and behavioral analytics in order to help stakeholders authenticate and manage their digital identities, and to create additional value for enterprises.
- **CISO expertise in security and privacy will help improve digital inclusion**—Security and privacy are at the core of digital identities and digital inclusion. CISOs will play an important role in addressing issues at enterprise, industry, national and global levels to provide secure digital identities.

For questions about the Accenture Cybersecurity Forum Women's Council, please contact **Valerie Abend** or **Lisa Harris**.

CONTACT

Valerie Abend
Managing Director,
Accenture Security

Accenture Cybersecurity Forum
Women's Council Chair

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 469,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organizations' valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.

Visit us at www.accenture.com

Follow us @AccentureSecure

Connect with us