accenturesecurity

ACCENTURE CYBERSECURITY FORUM

A perspective on the “post-digital era” and security: Five future trends

Virtual Roundtable Summary

April 17, 2019

DISCUSSION

Based on member input, the Accenture Cybersecurity Forum (ACF) convened a virtual roundtable, "A perspective on the 'post-digital era' and security: Five future trends," on April 17, 2019. CISOs and senior security executives from multiple industries and organizations joined the discussion with guest subject-matter experts Michael Biltz, managing director – Accenture Technology Vision, Accenture Labs; and Lisa O'Connor, managing director – Accenture Security and cybersecurity research and development, Accenture Labs. The session was hosted by ACF Co-chair Andy Vautier, Accenture CISO.

The lightning speed of change, driven by technology, is taking us from the digital age toward a new reality, one Accenture calls the post-digital world. In the Accenture Technology Vision 2019 survey of business and IT executives, 45 percent of respondents reported that the pace of innovation in their organizations has significantly accelerated over the past three years due to emerging technologies. The survey report delivered several strong messages to CISOs about the importance of ecosystem-wide security and collaboration.

With that as a backdrop, ACF members explored how they can promote cybersecurity in a post-digital environment.

The roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers or participants is revealed.

Perspectives

Vautier introduced the Accenture Technology Vision 2019, “The post-digital era is upon us: Are you ready for what’s next?” The report highlights five trends:

1. **DARQ Power**
   Understanding the DNA of distributed ledger technology, artificial intelligence, extended reality, and quantum computing
2. **Get to Know Me**
   Unlock unique consumers and unique opportunities
3. **Human+ Worker**
   Change the workplace or hinder the workforce
4. **Secure US to Secure ME**
   Enterprises are not victims, they’re vectors
5. **MyMarkets**
   Meet consumers’ needs at the speed of now

He singled out two trends that are particularly relevant to enterprise security executives: new technologies that are catalysts for change (DARQ Power) and enterprises as security co-players and collaborators within an increasingly risky ecosystem (Secure US to Secure ME).

DARQ power

Biltz noted that $1.1 trillion was spent on digital transformation in 2018. More than 90 percent of enterprises are undergoing a digital transformation, and the majority of those report that their efforts are relatively mature. The cloud, analytics, and social and mobile technologies have become ubiquitous in the last five or six years.

“What does it mean if every company is a digital company?” Biltz asked. “We are entering a post-digital era where the bar is being raised in terms of technology within the enterprise.” He cited several examples of companies applying technology in new ways, such as:

- An automaker is “capturing moments” on the shop floor to help workers do their jobs, and 3-D printers are being used to build tools on demand to address immediate challenges.
- Applying the principles of personalization, a healthcare company can now create a “digital twin” of a patient’s heart that surgeons can analyze to improve outcomes while the patient is being treated.

Eighty-nine percent of businesses are already experimenting with one or more DARQ technologies, expecting them to be key differentiators, according to the Accenture report. DARQ technologies have significant potential to help enterprises know their customers, create unique digital identities, personalize offerings and compete in a market of one. “DARQ technologies can deliver new ways of creating value and building customer loyalty, but they also raise new privacy and security challenges,” Biltz declared.

Strategically, DARQ technologies will transform the agility of an enterprise in a variety of ways, including serving customers, leveraging partners and refining the value chain. “Cybersecurity approaches must respond to changes that will take place more rapidly than ever across the enterprise ecosystem, not just within the confines of the enterprise,” he said.

Are CISOs prepared to manage the cybersecurity risks spawned by emerging DARQ technologies? “We’re part way there,” O’Connor declared, “but AI is posing a whole set of new challenges. AI presents a novel attack surface that hasn’t been fully explored. For example, can we trust the data after it's been installed? If you think of technology adoption as 'crawl-walk-run,' we're just starting to walk when it comes to AI-related cybersecurity." She urged CISOs to be "brilliant custodians" of data. "We have to protect the fuel that powers AI."

Biltz added that the issues of data integrity, accuracy, confidentiality, security and management have become security concerns, and are no longer primarily of concern only to the people creating and analyzing the data.

O'Connor pointed to the challenge of explaining the implications and risks of a post-digital environment to boards of directors. She recommended that CISOs carefully consider how to explain DARQ technologies to board members to enable them to understand the opportunities and challenges of these innovations. "We're all familiar with the effort required to educate board members about the migration to digital. When we look at DARQ technologies and ecosystem risks, we have a much bigger challenge on our hands. CISOs will have to help boards get over a huge learning curve."

CISOs shared varying perspectives on their ability to manage the cybersecurity risks posed by new technologies. One CISO said his company is trying to understand all the implications of adopting DARQ technologies, but is not sure it is fully prepared yet. Other members reported that managing cybersecurity risks across their ecosystems is an emerging priority. As their organizations make strides in digital transformation, it is essential to examine how to compete securely in a post-digital world.

Ecosystem security and privacy risks

Eighty-five percent of business and IT executives surveyed for the Accenture Technology Vision 2019 agreed that integration of customization and real/neartime delivery is the next big wave of competitive advantage. “It’s not just Amazon or Google that are at risk,” Biltz observed. “Every company will be changing the way it interacts with customers and employees, and the implications for security, ethics and society must be considered.”

Furthermore, 87 percent of survey respondents believed that to be truly resilient, organizations must rethink their approach to security in a way that defends not just themselves, but also their ecosystem.

Roundtable participants agreed that managing third-party risks is one of the most challenging aspects of their ecosystems. A variety of best practices emerged from the discussion about how CISOs can secure increasingly exploitable ecosystems.

O’Connor stressed the importance of “reframing risk” to account for ecosystem relationships, and proactively making security a part of business discussions. CISOs should broaden their perspective of their enterprise ecosystem and consider cybersecurity risk within their industry sector and their customer, supplier and adjacent domains. “Risk exposure now extends from within the enterprise to across your industry and across your supply chain. As the Mirai and Satori attacks have shown us, our reliance on connectivity requires CISOs to focus on broader borders.” She cited the example of an organization that engaged two universities in a threat modeling exercise that revealed 147 risk scenarios the organization had not previously considered.

O’Connor pointed to the challenge facing the financial services industry. “While companies within the sector have done a good job of establishing standards and practices, they may be dependent on others outside that ecosystem—companies that are not in their industry—that don’t share the same cybersecurity culture. We need to extend the boundaries of our defenses to those outliers.”

A CISO stressed the importance of consistent risk mitigation requirements and capabilities across complex, matrixed enterprises to establish a common baseline. Another member asserted that managing cybersecurity risk may require CISOs to spend as much time helping third parties manage risks as they do people within their own enterprise. Another participant suggested that because partners are at different levels of maturity, it is important to get the fundamentals right, understanding partners' risk profiles and assisting them where possible.

A CISO reported that his company is making an effort to ensure that its data is as secure across its supply chain as it is within its premises. He urged other CISOs to start by reaching out to trusted partners to identify best practices and learn what solutions partners are using.

Biltz declared that third parties should be "partners in compliance," and recommended collaborative "co-policing" to ensure effective risk mitigation.

He added, "Companies tying their systems more closely with their partners will be starting to shape the way we work and live. That will bring an enormous amount of opportunity, but also important questions" about ensuring security, addressing ethical issues and defining societal good. "In the post-digital era, the winners and losers will be determined by how they handle security and privacy."

Conclusion

Summing up the discussion, Vautier said that companies will be competing based on how they securely and effectively apply DARQ technologies; unlock unique customer opportunities; rapidly meet consumer needs; empower the workforce with new technology; and manage cybersecurity risks across the entire enterprise ecosystem. "In that sense, the CISO can become a business differentiator."

He added, "The point raised by one of our CISOs that his company spends as much effort securing its ecosystem as it does securing the enterprise should give us all pause. We need to internalize that companies will live or die based on how well they manage the boundaries among security, transparency and privacy across their ecosystem."

CONTACT US

Andy Vautier

Accenture CISO
Accenture Cybersecurity Forum Co-chair

John Valente

3M CISO
Accenture Cybersecurity Forum Co-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 477,000 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 us at **www.accenture.com/security**

Visit us at www.accenture.com

Follow us @AccentureSecure

Connect with us

accenturesecurity

ACCENTURE CYBERSECURITY FORUM

A perspective on the “post-digital era” and security: Five future trends

Virtual Roundtable Summary

April 17, 2019