accenturesecurity

ACCENTURE CYBERSECURITY FORUM

Securing the digital economy: Reinventing the Internet for trust

Virtual Roundtable Summary

February 6, 2019

Based on member input, the Accenture Cybersecurity Forum (ACF) convened a virtual roundtable, “Securing the digital economy: Reinventing the Internet for trust,” on February 6, 2019.

Accenture, with the support of the ACF, conducted research to explore the issues of digital trust and digital security. Following a presentation at the World Economic Forum Annual Meeting in Davos, the research report was shared with ACF members in advance of the roundtable. The report recommends that CEOs pursue business initiatives in three areas—governance, business architecture and technology—in order to secure a trustworthy digital economy.

CISOs from multiple industries and organizations joined the call to discuss the research findings and explore ways to elevate trust and security in their enterprises’ business strategies. Our subject-matter expert for the roundtable was Kelly Bissell, Senior Managing Director – Accenture Security and co-author of the research report. Our hosts were ACF Co-chairs Andy Vautier, Accenture CISO, and John Valente, 3M CISO.

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.

Vautier began the discussion by noting that the topic of the research is highly relevant. As CISOs, “we wrestle daily to deliver incremental cybersecurity improvements across people, processes and technology” within a landscape filled with increasingly severe risks that threaten to outstrip any government’s or institution’s ability to respond. CISOs are challenged to counter cybersecurity threats and build trust while relying on Internet technology that was not designed with security at the forefront.

DISCUSSION

“For several years, we’ve all been looking at well-intended but incremental approaches,” Vautier continued. “Some progress has been made, but what’s needed now are disruptive thinking and disruptive approaches. Driving disruptive thinking may be difficult, but it is what is required. The ideas in this study may hold some of the keys to the change that we need as a community of security leaders.”

Valente agreed with the call for more disruptive thinking. “It is the enterprises that use the Internet that must focus on these issues in greater detail,” he added. With increasing complexity in the use of technology and social media within the enterprise, CISOs must concentrate on governance and business architecture.

The Accenture research report reinforces the value of disruption. While 68 percent of CEOs responded that their businesses’ dependence on the Internet is increasing, they acknowledged that their confidence in Internet security, already low at 30 percent, will drop even lower if nothing changes to improve it. In the next five years, the confidence level in the Internet is forecast to drop to 25 percent, while dependence on it is assumed to remain at 100 percent.

Bissell warned, “While the Internet is not necessarily broken, it is really fragile.” For companies that have Internet technology at the core of their value proposition, building stakeholder trust and securing the digital economy are imperative. A CEO told Bissell at the World Economic Forum Annual Meeting, “We are becoming a technology company, but without trust, our customers will go elsewhere.”

“CEOs are concerned that innovative technologies are outpacing the ability of governments or their own enterprises to maintain stakeholder trust,” Bissell revealed. This concern was underscored in discussions about global risk at Davos, where CEOs said cybersecurity was second only to climate-related impacts as a top risk concern.

Bissell offered a number of recommendations for how CEOs and CISOs can build a trustworthy digital economy and secure Internet:

1) Help establish industrywide standards and best practices.

2) Forge collaborative relationships with peers, government representatives, regulators and industry associations.

3) Embed the idea of a trustworthy digital economy in the vision of their company's business architecture.

4) Ensure that security is a high priority within their company and throughout its ecosystem of partners, suppliers and end users. "It's typical that CISOs don't have control over cybersecurity among suppliers and vendors, and that may have to change," he said.

He reminded the group that "no one can solve these issues on our own. This is an area where we have to bond together as a market." He suggested that the World Economic Forum, with its composition of CEOs, regulators and law enforcement, may provide a means of collective action.

Governance

Bissell maintained that improving governance requires establishing industry codes of conduct, principle-based standards and policies for consumer control of digital identity, as well as making a commitment to rapid sharing of information among enterprises when they have been breached. "Musician will.i.am spoke at Davos and predicted a groundswell of consumer demand for control of their identities and data," Bissell reported. "Enterprises need to get ahead of the curve."

He also stressed the importance of greater CISO representation on boards of directors, adding, "If your enterprise is becoming a tech company, your board needs to reflect that transformation."

A CISO brought up the need for governance that includes cultural change—removing the "sludge" inside the enterprise that inhibits a culture of cybersecurity. He said many CEOs are not sufficiently focused on driving the significant effort required. "Companies that have been breached are more directed to address the required culture change," he asserted. "But companies that haven't been breached must get more focused before they have to learn the hard way."

A member added that there is a lot of pressure from the asset management community about cybersecurity. "This is definitely the right time for CISOs to get the attention of the board and CEO," she said. "CISOs should be making more presentations to the board, and there should be greater discussion about technology talent and technology's strategic implications."

Valente observed that CISOs are quite good at finding security vulnerabilities, but need improvement in "aggregating and explaining risks in ways that leaders can understand."

Having the CISO report to someone other than the CIO is one way of refining governance and elevating the cybersecurity discussion, said Bissell. "Right now, if the CIO has a cybersecurity budget, they're more likely to spend it on bells and whistles."

Building on that point, a CISO added that she and her company's CIO got different questions at a recent board meeting. "We're not asking the CIO what they're doing to make the business more secure, and we're not asking the CISO how to grow the business."

Vautier remarked that the discrepancy is often a matter of accountability and rewards. "Linking compensation to security is a very effective way of driving security accountability," he said.

Another CISO offered ideas for governance. “There are opportunities for corporate entities to improve the way we work with suppliers, and perhaps to jointly invest in developing what might be called a more secure Internet 2.0. We should be working with friendly governments on regulatory harmonization. But I think there is little hope of engaging with national bad actors. They are going to continue to work in their own best interests. It will be difficult to establish international norms of behavior.”

Business architecture

To ensure a trustworthy digital economy, according to the Accenture report, CEOs need to embed security into their business architecture—the company’s business model and value chain, including its leadership structure. The digital economy is fostering new business architectures in which trust is a critical component.

A CISO participating in the roundtable described trust as a monetary factor as enterprises collect massive amounts of data about consumer behavior, even as consumers get more educated about the risks. “More companies are using analytics to improve their products or data mining to generate revenue and drive new growth. But consumers are getting more sensitive about personal data. We have to recognize that consumer trust is an easy thing to break.”

Competition in the digital economy is reshaping the responsibilities of the CISO and the rest of the C-suite. In a competitive environment where CEOs and CISOs are expected to innovate quickly, a CISO said, “We need to get everyone in the same boat, so that the CISO can also support business goals and objectives and the rest of the enterprise can support the need for greater security. I don’t think we’re asking both groups to address both problems.”

Bissell pointed to a best practice of holding line of business leaders accountable for cybersecurity, “so the CISO isn’t always left holding the bag.” A major financial services firm added a security element to its bonus structure, and “those line of business leaders now have skin in the game when it comes to cyber risk.”

Technology

According to the Accenture report, 79 percent of business leaders said the rate of technology adoption and innovation has outpaced the security features needed to ensure a resilient digital economy.

Bissell noted, “We need to push vendors to improve security within their functions and products.” The Accenture report urges CEOs who oversee technologies powering and protecting the Internet to deliver more secure solutions for the Internet’s basic protocols, devices, advanced networking and computing.

Valente discussed the potential fragmentation of the Internet, whereby China or Russia or other nation states may create a version of the Internet that serves their proprietary interests. Another CISO added her concern that the rise of nationalism around the world could result in a fragmented Internet. Such action could pose significant business risk, particularly relating to intellectual property protection.

A participant declared that enterprises cannot rely on technology alone to solve cybersecurity problems. “Whatever we come up with today will continue to evolve, so an overreliance on technology is risky.” She called for a balanced approach, including cultural change, governance and business architecture. She added that CISOs should recognize that AI and machine learning, while they have value, “might also be weaponized against us.”

Bissell conveyed the ideas he shared with CEOs at Davos. He emphasized the importance of investing in technology that will reinforce trust and “actually move the needle” in terms of cybersecurity. In addition, he recommended that CEOs elevate the role of the CISO and deepen their own understanding of technology. “Yes, the CISO needs to be bilingual, but so does the CEO.” Bissell urged CEOs to “encourage agility in their organizations to address security issues more quickly.”

Conclusion

Securing the digital economy with a foundation of trust will require advancements, and even disruption, in three areas: governance, business architecture and technology. Governance must be improved through such initiatives as industry codes of conduct, principle-based standards, consumer-controlled digital identities and a commitment to sharing information after breaches. New business architectures will emerge as enterprises prioritize security by design, line of business leaders share accountability for cybersecurity with CISOs, more CISOs are put on boards of directors, and cybersecurity efforts extend across the entire enterprise value chain. Advances in technology, including resolving the vulnerabilities inherent in current Internet protocols, heightening security at the edge and embracing secure software-defined networking, will also help.

“We firmly believe we have to address all three things at one time,” Bissell emphasized. “Groups like the Accenture Cybersecurity Forum and the World Economic Forum … have more voice to influence CEOs, vendors, and regulators” than any single enterprise. He encouraged ACF members to help identify the most important issues requiring further research, and to engage with the World Economic Forum Centre for Cybersecurity to collectively address key cybersecurity questions.

Valente agreed that the complex issues discussed during the roundtable cannot be solved individually. There are multiple organizations within which CISOs can work to address the issues of governance, business architecture and technology. He added, “We need to push vendors and regulators in directions that will help us.”

Vautier was encouraged that CISOs agreed that cybersecurity issues should be addressed collectively. He proposed that the ACF revisit the issue of securing the digital economy at some point in the next six months for a read-out of progress made in developing a roadmap.

CONTACT US

Andy Vautier
Accenture CISO
Accenture Cybersecurity Forum Co-chair

John Valente
3M CISO
Accenture Cybersecurity Forum Co-chair

ABOUT ACCENTURE

Accenture (NYSE: ACN) 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 us at **www.accenture.com/security**

Visit us at www.accenture.com

Follow us @AccentureSecure

Connect with us