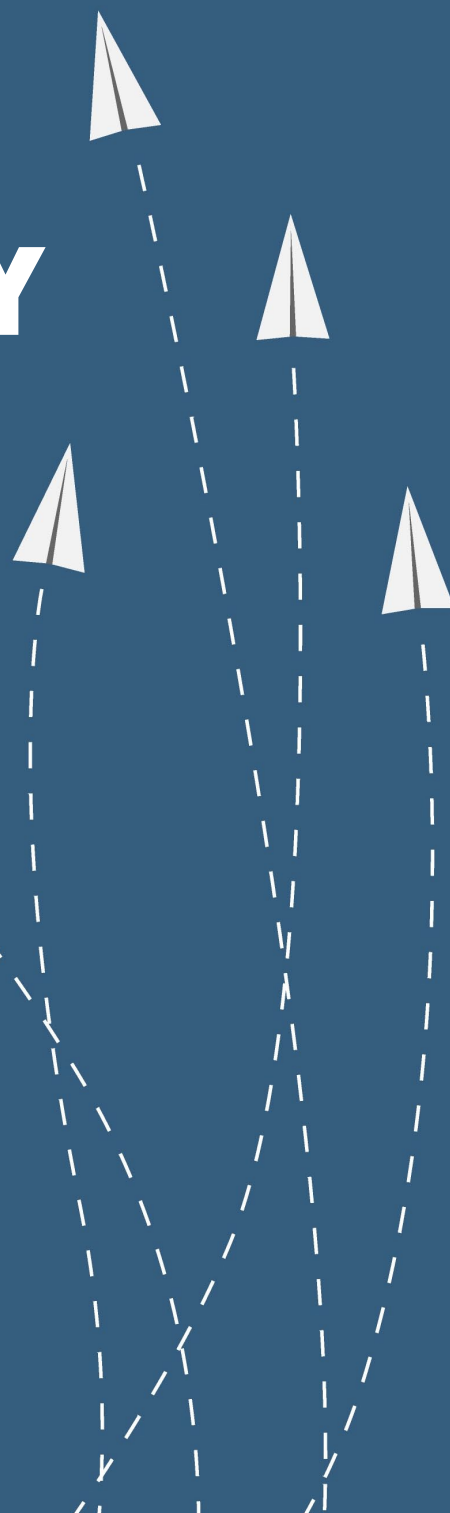
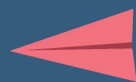


# ACCENTURE CYBERSECURITY FORUM

## THE CHALLENGE OF PARTNERS AND THIRD PARTIES: SECURING THE ENTERPRISE ECOSYSTEM

VIRTUAL ROUNDTABLE SUMMARY

NOVEMBER 12, 2019



## **DISCUSSION**

**On November 12, 2019, the Accenture Cybersecurity Forum (ACF) convened a virtual roundtable, “The challenge of partners and third parties: Securing the enterprise ecosystem.” CISOs from multiple industries and organizations joined the call to discuss approaches to maintaining strong third-party cybersecurity.**

The job of securing the enterprise is complicated by third-party vulnerabilities. Identifying and addressing the major security risks posed by third-party partners is a top CISO priority.

Our subject-matter experts for the call were an information security executive at a multinational financial services company; and Nick Taylor, Accenture Security managing director, United Kingdom/Ireland lead and global strategy and risk lead. The session was hosted by ACF Chair Andy Vautier, Accenture CISO.

The roundtable was conducted under the Chatham House Rule: All 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 began the discussion by noting that threat actors are pivoting toward attacking third parties as a means of breaching enterprise targets. In response, Accenture actively assesses risks and rejects prospective partners that lack the appropriate security posture. The company also has a team that responds to client requests for information about Accenture’s own cybersecurity efforts. Like many other large enterprises with thousands of third-party providers, Accenture focuses on mitigating cybersecurity risks among its most important third parties, while addressing all partners.

## DISCUSSION

### Current approaches

Members shared a variety of approaches they are taking to minimize third-party risk. Most notably, they agreed that insufficient resources, the complexities of global supply chains, the regulatory demands of various regions or countries, and other factors make third-party cybersecurity a difficult challenge.

Risk tiering is a common practice. Many organizations vary the resources and assessments they apply to individual third parties depending on the level of risk a partner presents. A multifaceted approach that categorizes vendors into tiers depending on risk level, type of data and nature of services provided is applied on an ongoing basis and combined with insights from onsite visits, questionnaires and scorecards.

Vautier reported that Accenture applies a robust risk assessment process to its portfolio of 10,000 suppliers relative to the work they perform for the company, the data types they use, the level of access they have and other factors.

Suppliers whose security posture is not consistent with the activities they are going to perform are rejected. Accenture focuses its greatest efforts on its top 50 risk-tiered suppliers.

Risk management is to some extent a function of industry. Some organizations focus primarily on customers, others on regulatory requirements.

Third-party risk management services such as CyberGRX, SecurityScorecard and BitSight can be helpful, but by themselves are not sufficient, according to several CISOs. These services are perhaps best regarded as part of a larger intelligence process.




CISOs are also addressing their roles as third-party providers to other organizations. A growing number of customers want to conduct tests of enterprise networks.

## DISCUSSION

### Major challenges in mitigating third-party risks

Taylor summarized six key challenges in maintaining third-party security: operating model, technical, operational, behavioral, benchmarking and legal. No single questionnaire, technology solution or third-party stress test can provide complete due diligence across all dimensions.

### THIRD PARTY SECURITY KEY CHALLENGES

<b>OPERATING MODEL CHALLENGES</b>	 <b>SUPERFICIAL CHANGE MANAGEMENT</b> Supplier assurance is often not embedded into enterprise change management and supplier onboarding framework	 <b>LACK OF UNIFIED INTERACTION</b> Business teams are constantly bombarded by duplicate requests to complete similar type of assessments (e.g. internal audits, SOX assessments)	 <b>GOVERNANCE</b> Clear and codified ownership and accountability is key in ensuring an effective oversight of supplier assurance
<b>TECHNICAL CHALLENGES</b>	 <b>CLOUD ADOPTION</b> Enterprises experience an average of 23 cloud related threats monthly, yet there is limited cloud-specific security assessment frameworks.	 <b>TECHNOLOGY INFANCY</b> Third party security assessment still relies on spreadsheet-based questionnaire without integration of advanced intelligence or machine learning elements	 <b>INDUSTRY SHARING</b> Many businesses operate cross-clients and may have been previously audited. Ability to leverage such information cross-industry will foster efficiency
<b>OPERATIONAL CHALLENGES</b>	 <b>SCHEDULING &amp; CAPACITY CONSTRAINT</b> Beyond IT team, business resources are increasingly assigned additional responsibilities of completing security assessments.	 <b>MANAGEMENT INFORMATION &amp; SLA</b> Absence of management information system and defined SLA often translates into significant lags in obtaining assessment responses	 <b>DECENTRALISED MANAGEMENT</b> Businesses running at global scale often decentralise their operations, diminishing the ability to maintain a centralised view and control of all their third party networks
<b>BEHAVIOURAL CHALLENGES</b>	 <b>MINIMAL INCENTIVES &amp; PENALTIES</b> Without clear and tangible incentives and consequences, third parties are often reluctant to take initiatives in enhancing their security resilience	 <b>SECURITY AWARENESS</b> Awareness programs are often not realised in small businesses. Ponemon study shows that even the least effective training has 700% return on investment	
<b>BENCHMARKING CHALLENGES</b>	 <b>NO DEFINITIVE INDICATOR/ SOLUTION</b> The fast paced cyber threat landscape means there has not been any single ultimate solution or indicator of companies' resilience in facing cyber attacks	 <b>UNINFORMED PROCUREMENT</b> Procurement teams are often not data security-literate to take an informed judgement based upon the company's wider data security strategy	 <b>NO VISIBLE VALUE, NO FUNDING</b> Funding follows the visible prospects of tangible outcomes. Unfortunately it is often impossible to demonstrate third party risk reduction until remediation is underway
<b>LEGAL CHALLENGES</b>	 <b>CONTRACT GAPS</b> The need to understand what the business requires from the third party and ensure that this is mapped into the contract.	 <b>CROSS-BORDER ASSURANCE</b> Many organisations operate across multiple jurisdiction which requires understanding of territorial legitimacy in exercising lawful third party security assessments	

Participants discussed the challenge of building a comprehensive list of their enterprise's third parties. Taylor suggested using a combination of data to see the broad landscape of partners. For example, the procurement database, general ledger and record of where things are bought can help CISOs understand where their third parties are.

Concerns now extend to fourth-party relationships. Governance issues such as ownership and management responsibilities for third parties need to be

## DISCUSSION

sorted out between the CISO and the rest of the business. Movement of data and operations to the cloud, particularly hybrid cloud models, is creating new exposures. Assessing the impact of third-party business decisions, such as moving operations offshore, puts additional strain on limited resources.

### Best practices

Given finite cybersecurity resources, CISOs must prioritize their efforts and protect “the crown jewels” of the enterprise. ACF members suggested several key steps CISOs should take:

- Bake cybersecurity into your information architecture by engaging the owners of business processes, procurement, legal and other stakeholders in quantifying risks and setting priorities.
- Incorporate cybersecurity compliance into third-party contract provisions.
- Assess and address risks throughout the lifecycle of third-party relationships, not only at onboarding but also at renewal and offboarding.
- Automate compliance as much as possible.
- Consider the potential biases of third parties and people in the enterprise doing assessments. Try to identify claims that may require verification. Taylor stressed the importance of business engagement, noting that he has seen a 700 percent return on investment in training people in the business about identifying and mitigating vendor risks.
- Don’t wait for a “silver bullet.” Recognize that no tool, process or outside assessment can completely address cybersecurity risks. While each may provide valuable data points, CISOs should strive for the combination that is right for their enterprise. It is an art, not a science, to combine and effectively use information.

## DISCUSSION

- Use risk tiering. Engage the business in identifying the “crown jewels” and third parties that could pose a significant risk. This might mean focusing on the top 10 percent of third parties to enforce cybersecurity compliance; don’t try to conduct the same due diligence with every vendor. Ask your business colleagues, “Which third parties affect your operations the most? Who are the top suppliers in your value chain?”

## CONCLUSION

In closing, Vautier affirmed the value of a data-driven, business-focused, tiered-risk approach to secure the enterprise ecosystem. Taylor recommended expressing third-party risk in business language—such as where your major business risks lie and which third parties are involved in those business processes—in discussions with leadership.

## CONTACT

### ANDY VAUTIER

Chief Information Security Officer,  
Accenture  
Chair, Accenture  
Cybersecurity Forum

## 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 482,000 people serving clients in more than 20 countries, Accenture drives innovation to improve the way the world works and lives.

Visit us at [www.accenture.com](http://www.accenture.com).

## ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently drive 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 [www.accenture.com/security](http://www.accenture.com/security).

Visit us at [www.accenture.com](http://www.accenture.com)



Follow us @AccentureSecure



Connect with us