



M&A and Cybersecurity

Accenture Cybersecurity Forum
Global Executive Leadership Network

July 11 2023
Session Summary



From the Accenture Leadership

ACF members came to this Forum about M&A with a host of questions. What is the CISO's role during the due diligence phase? What high priority security domains are other organizations focusing on post close? How can we maintain good identity management and access control in the early stages of an integration?

Our two guest cybersecurity subject matter experts shared their deep and practical experience across a variety of steps in the transaction process. We thank them for their participation.

Thank you as well to those who participated in the roundtable discussion. We hope you find the perspectives and best practices that emerged from the conversation useful as you support mergers and acquisitions with sound cybersecurity practices.

Cheers,



Paolo Dal Cin

Global Head of Accenture Security
ACF Executive Sponsor

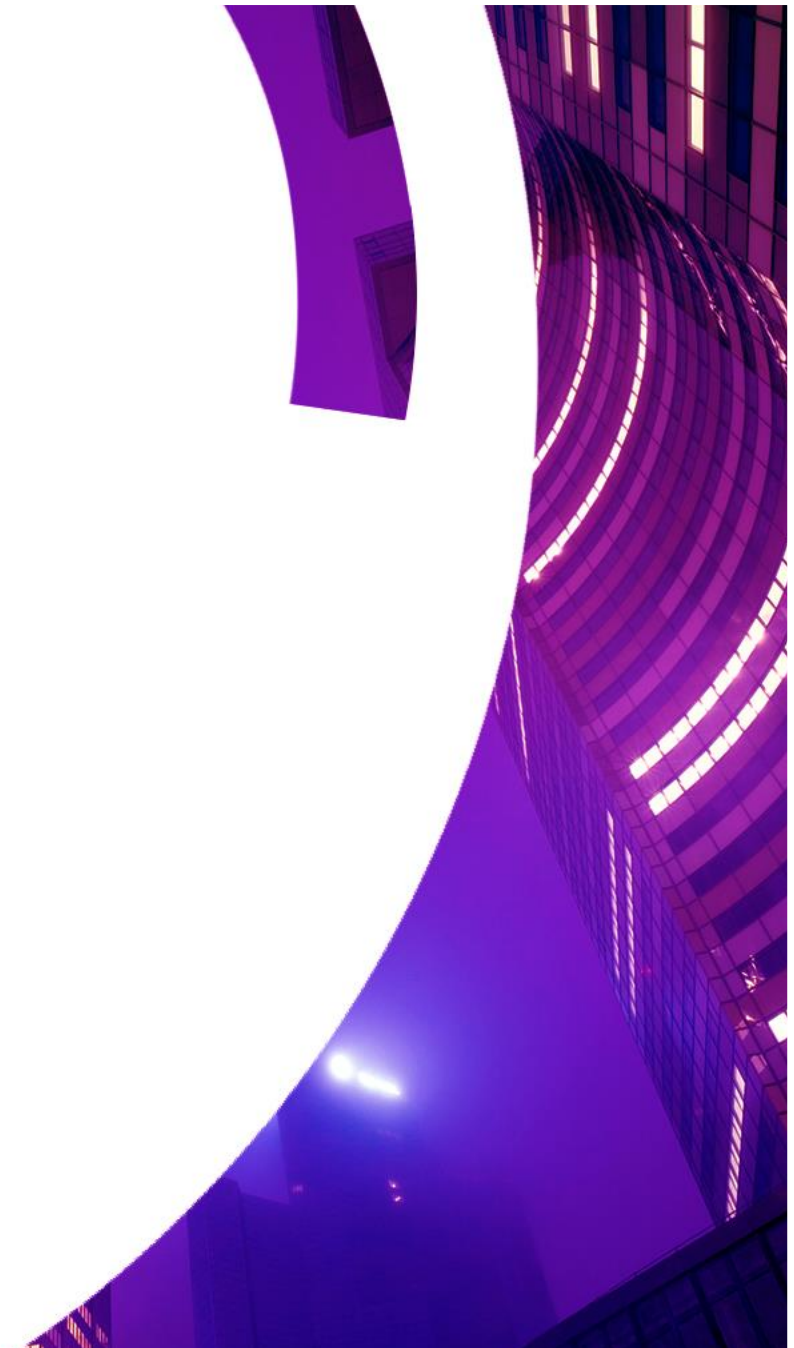
[LinkedIn](#)



Kris Burkhardt

Accenture CISO
ACF Chair

[LinkedIn](#)



M&A and Cybersecurity



The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “M&A and Cybersecurity” on July 11, 2023.

Forum members have expressed interest in examining cyber defense issues and the role of the CISO organization during negotiation, due diligence, deal closing and post deal integration for both mergers and acquisitions. Are there any best practices we should follow?

This 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, nor participants, is revealed.

In this summary:

[Due diligence >](#)

[Post deal >](#)

[Integration >](#)

[The Board’s perspective >](#)

[Best practices >](#)



“Have a general estimate and refine it over time.”

— Subject Matter Expert

Due diligence

Typical due diligence questionnaires are rarely adequate in assessing a target company’s cybersecurity risk profile, said a subject matter expert. Collect evidence that the acquisition target has baseline controls in place (i.e. MFA, credentials reset, remote patching). Penetration testing may be called for to actually confirm a company’s security posture.

The human factor is of critical importance. Both subject matter experts stressed the need for transparent communications so that both sides agree on expectations and responsibilities.

Since the cybersecurity function is typically considered a cost center, it pays to set aside budget upfront to pay for investments and remediation, as well as identify opportunities to reduce redundancy (i.e. tools contracts). A subject matter expert described the initial budgeting process as similar to selecting a tee-shirt which range in sizes from small to extra-large. “Have a general estimate and refine it over time,” the subject matter expert said.



“You should demand full disclosure, and quickly establish accountability to rapidly prioritize and mitigate risks.”

— Subject Matter Expert

Post deal

While cybersecurity concerns are not likely to undermine a deal, risks and costs must be considered. “You should demand full disclosure, and quickly establish accountability to rapidly prioritize and mitigate risks.

“Threat actors who understand the concept of one-to-many will look at a deal as an opportunity to exploit vulnerabilities,” said a subject matter expert. “If they successfully exploit a ransomware attack on the acquired company with a less mature security posture, there could be a multiplier effect. They will be encouraged to look for other opportunities.” An ACF member added: “By acquiring a less cyber-mature company, the mothership may become a profitable target.”

That kind of risk underscores the importance of rapid risk mitigation. But CISOs should also appreciate that company leadership on both sides of a deal can feel overwhelmed. “It’s a time for diplomacy and partnership,” said an ACF member.



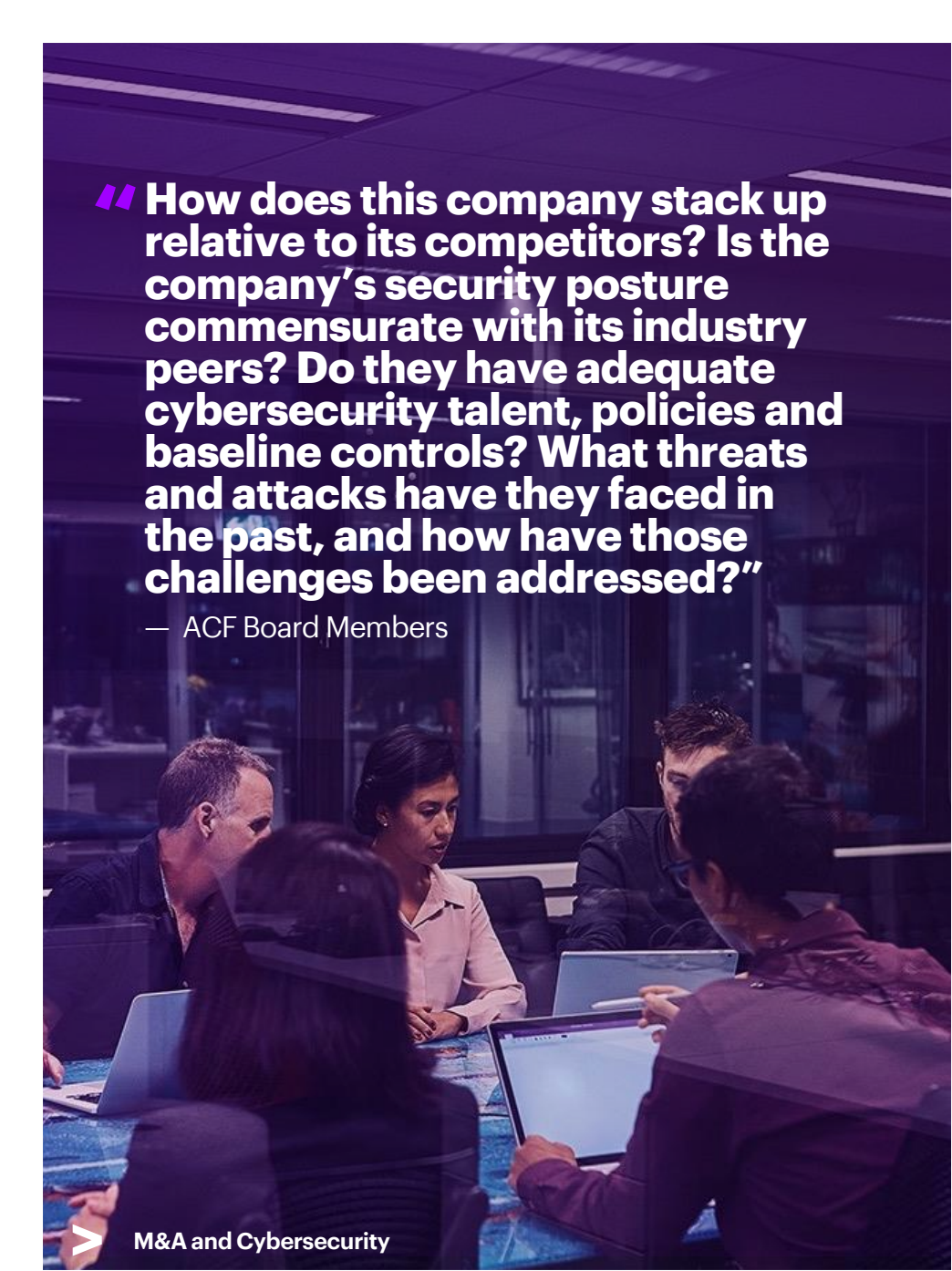
“ ... we saw that acquisitions were dragging their feet. We adjusted our approach and developed an acquisition cyber enablement program that includes a framework, playbook and a dedicated team of IT and cyber professionals.”

— Subject Matter Expert

Integration

A subject matter expert who has managed dozens of acquisitions said: “When we started out, we approached acquisitions about compliance the same way we did with our mature internal operation,” they said. “But we saw that acquisitions were dragging their feet. We adjusted our approach and developed an acquisition cyber enablement program that includes a framework, playbook and a dedicated team of IT and cyber professionals. We are there to support and make them successful, not leave them out on a ledge.”

Since integration can be a complex, be realistic about what can be accomplished within certain timeframes and understand the levels of risk the enterprise is willing to accept during each phase of the integration process. Integration priorities often include hardening legacy systems, mitigating high-risk vulnerabilities, measuring and reporting on progress and executing plans to deliver ongoing training to help people develop “muscle memory” of sound cybersecurity practices.



“ How does this company stack up relative to its competitors? Is the company’s security posture commensurate with its industry peers? Do they have adequate cybersecurity talent, policies and baseline controls? What threats and attacks have they faced in the past, and how have those challenges been addressed?”

— ACF Board Members

The Board’s perspective

ACF members who serve on boards said board members need to ask the right questions. How does this company stack up relative to its competitors? Is the company’s security posture commensurate with its industry peers? Do they have adequate cybersecurity talent, policies and baseline controls? What threats and attacks have they faced in the past, and how have those challenges been addressed?



“The M&A playbook should include explicit plans for how the two parties will communicate and work through issues and expectations.”

— ACF Best Practice

Best practices

- **Cultivate transparency and relationships**—The M&A playbook should include explicit plans for how the two parties will communicate and work through issues and expectations.
- **Mitigate risks upfront**—The early days of a deal close can make a company an attractive target for threat actors.
- **Establish accountability**—Everyone involved should understand their role and what’s expected of them.
- **Governance should reflect the fact that each company and each deal are different**—You can’t always strongarm your way to compliance. Be flexible and find ways to work with people on the other side of the deal.
- **Be clear about the value of an acquisition**—Focus on risks specific to that deal rational. Understand if the deal is about IP, customers, or talent. If the goal, for example, is to acquire intellectual property, consider a dark web analysis for leaked information and detailed reports on breaches and other malicious behavior that might undercut the IP’s value. If customer acquisition is important, assess the extent by which the company’s cybersecurity strategy cultivates trusted relationships.
- **Provide tools and support, not just advice**—Even in cases where the full integration of systems or SOCs is not required, support the acquired company in adopting your security controls.



**“Let’s share what we know
to secure what we must.”**

— **Kris Burkhardt** Accenture CISO, ACF Chair

Work the network

Contact [our team directly](#)
for questions and member introductions.

About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organizations build their digital core, optimize their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent and innovation led company with 738,000 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology with unmatched industry experience, functional expertise and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Accenture Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients succeed and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities. Visit us at www.accenture.com

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Visit us at accenture.com/security.

Copyright © 2023 Accenture All rights reserved.
Accenture, and its logo are trademarks of Accenture.