DRILL INTO CYBERSECURITY WHEN CONSIDERING M&A DEALS
OIL AND GAS INDUSTRY

JUNE 2019
MERGERS AND ACQUISITIONS ARE ACCELERATING

There is interest in North America unconventional plays, such as BP’s 2018 acquisition of BHP’s assets.¹

The Permian Basin is leading the way, as we’ve seen with Occidental Petroleum’s 2019 bid for Anadarko.²

There is also activity in the downstream sector, such as Marathon Petroleum’s 2018 purchase of Andeavor.³

¹ BP press release: on.bp.com/2HUChl0
² Occidental Petroleum press release: bit.ly/2EOg436
³ Marathon Petroleum Corporation press release: bit.ly/2WKZ8ou
M&A execution was once limited to examining financial ledgers, inspecting equipment and evaluating plays.

But today’s M&As must have cybersecurity experts seated at the deal table.

That’s because cyber risk translates into monetary amounts. The media has reported on breaches (in other industries) that affected M&A deal values.

Cybersecurity protects M&A deal value by:

• Proving security rigor along the value chain: Information technology and operational technology (IT/OT) systems
• Delivering a better understanding of risks:
  • IT/OT convergence risk – operational technology feeds into information technology
  • Geopolitical risk – ‘significant rise in economic espionage’ by threat actors such as nation-states

1 Accenture’s Ninth Annual Cost of Cybercrime Study: https://accntu.re/2WuxFH
Cybersecurity is essential throughout the M&A lifecycle.

**PHASE 1: PRE-DEAL**
- Threat Intel
  - 1A
- Threat Hunt
  - 1B
- Penetration Test
  - 1C

**PHASE 2: DURING TRANSACTION**
- Remediation Activities
  - 2A
- Secure Communication
  - 2B
- Day 1 & Transition Planning
  - 2C

**PHASE 3: DAY 1**
- Security Culture Transformation
  - 3A
- Process Alignment
  - 3B
- Platform Rationalization
  - 3C
PRE-DEAL CYBERSECURITY IDENTIFIES RISKS

ACTIONS

**THREAT INTEL**
Gain an understanding of the potential threat landscape via the dark web and other Internet sources.

**THREAT HUNT**
Conduct proactive analysis across IT/OT systems throughout the target and the parent environment to identify indicators of compromise, tactics, techniques and procedures.

**EXTERNAL PENETRATION TEST**
Test the external perimeter to identify vulnerabilities across the M&A target’s environment.

**Did you know?**
Intellectual property could already be out on the internet or the dark web.
CYBERSECURITY DURING M&A TRANSACTION

ACTIONS

REMEDIATION ACTIVITIES
Cyber risks identified during the pre-deal activities should be addressed in this phase.

SECURE COMMUNICATIONS
Work with organizations who can provide an integrated and secure communications infrastructure to ensure confidentiality.

DAY 1 & TRANSITION PLANNING
Define set of cybersecurity capabilities for Day 1 and implementation plan for integration of people, processes, and technology.

Did you know?
‘Humans are still the weakest link’ in cybersecurity.¹

¹Accenture’s Ninth Annual Cost of Cybercrime Study (2019): https://acncntu.re/2WuxhFH
DAY 1 CYBERSECURITY FOR THE NEW COMPANY

ACTIONS

SECURITY CULTURE TRANSFORMATION
Begin adoption of the desired security culture with a plan to incorporate talent into lifecycles and metrics.

PROCESS ALIGNMENT
Align leading security policies, processes, standards, procedures and guidelines between both organizations.

PLATFORM RATIONALIZATION
Consolidate the critical applications and security solutions for the new enterprise such as identity and access management; governance, risk, and compliance; operational technology; pluggable authentication modules; and security information and event management.

Did you know?
Cybersecurity is everyone’s responsibility.¹

¹ Accenture’s Ninth Annual Cost of Cybercrime Study (2019): https://accntu.re/2WuxhFH
CONTACT US TO LEARN MORE

Edwin Cisneros
Managing Director
Accenture Security
edwin.cisneros@accenture.com

Jeffrey T. Miers
Managing Director
Accenture Consulting
jeffrey.t.miers@accenture.com

Copyright © 2019 Accenture. All rights reserved.
Accenture, its logo, and New Applied Now are trademarks of Accenture.