Welcome To The 10th Annual Hacking Conference

Dungeons and Dragons™

InfoSec Master Edition

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter

Security Considerations During M&A

November 6, 2023

westMONROE

INTRODUCTIONS

CHRISTINA POWERS
Partner, Cybersecurity
Los Angeles

DEAN RODIL
Senior Manager, Transaction Services / Cybersecurity
Chicago

As organizations continue to evolve, attackers are also evolving their tools, tactics, and procedures (TTPs) to hit organizations where it hurts most

ENVIRONMENTAL CHANGES

CYBERWARFARE *(Nation-State)*
CYBER RISK: Actors causing chaos and confusion for partners of high value competitors

SUPPLY CHAIN ATTACKS *(Nation-State & Cyber Crime)*
CYBER RISK: Compromise of partners for data exfiltration or ransomware

Shift to Remote Workforce
CYBER RISK: *Quick increase in publicly facing infrastructure footprint oftentimes at the cost of security posture*

Digital Transformation
CYBER RISK: Increased publicly facing digital footprint introduces additional attack vectors

Data Integration & Interoperability
CYBER RISK: Difficulty in securing sensitive data that is continuously in flux across environments

IT/OT/ICS/SCADA Isolation
CYBER RISK: Increased likelihood an attack impacts operations, revenue, and public safety

Big Data, A.I., and Machine Learning
CYBER RISK: Increased hoarding of data for analysis and insights requires additional safeguards

Monetization of Data *(Cyber Crime)*
CYBER RISK*:* Increased targeting of companies with valuable data

Monetization of Resources *(Cyber Crime) Crypto-jacking*
CYBER RISK: *Difficulty maintaining and validating accurate asset management*

Monetization of Availability *(Cyber Crime) Ransomware*
CYBER RISK: *Insecure cloud practices and poor incident response readiness may cripple an organization*

Ransomware & Public Data Exposure for Extortion
CYBER RISK*: Compounding pressure of extortion through attack of availability and breach of data if payment is not executed*

Cloud Adoption
CYBER RISK: Unclear cloud strategy and vision exposes gaps

The frequency and impact of cybersecurity events continues to increase

74%

of breaches involve the human element[1]

13%

Increase in average total cost of a breach from 2020 to 2023[1]

82%

Share of breaches that were cloud-based[1]

295

Average number of days to identify and contain a ransomware breach[1]

83%

Share of organizations that have had more than one data breach[1]

$5M

Average total cost of a critical infrastructure data breach[1]

277

Average number of days from data breach identification to resolution and restoration of service[1]

35%

of ransomware attacks involved the use of email[2]

[1]IBM Security, Cost of a Breach Report 2023
[2]Verizon 2022 Data Breach Investigation Report

A typical M&A transaction lifecycle will be comprised of multiple stages; cyber is typically a critical component in due diligence, hold, and exit stages

TRANSACTION LIFECYCLE

STRATEGY	DEAL EVALUATION		PRE-CLOSE	POST-CLOSE	
Strategy Development & Assessment	Target Selection	Due Diligence	Deal Structuring & Negotiation	Separation / Integration Planning	Separation / Integration Execution	Steady State / Hold	Exit

POTENTIAL WORKSTREAMS IN EACH PHASE OF THE LIFECYCLE

DEAL STRATEGY

- Business Case / Deal Thesis
- Market Assessment
- Search and Screen

TRANSACTION ADVISORY

- **Cybersecurity and Compliance Diligence**
- Technology Diligence
- Software Diligence
- Operations Diligence
- Digital Diligence
- Quality of Supply Chain
- Market / Competitive Diligence
- Carveout Diligence
- Merger Integration Diligence
- Sell-Side Advisory

DEAL EXECUTION

- Merger Integration
- Carveouts & Divestitures

PORTFOLIO VALUE CREATION

- **Third-party cybersecurity focused assessment conducted to identify/remediate security and operational gaps**
- Commercial Analytics
- Business Process Outsourcing
- Product Engineering
- Data Engineering, Analytics & Monetization
- Lead-to-Cash Transformation
- ERP Transformation

Note: Not Exhaustive

During the due diligence stage, acquisitions/transactions should incorporate activities and focus on identifying cyber, privacy, and compliance risks that could impede value creation

GENERAL CYBERSECURITY

- Confirm presence of security technical controls
- Examine operationalization of security controls
- Review business resiliency in the event of a security incident
- Assess security governance program

COMPILANCE

- Identify risks, exposure, and potential qualitative and quantitative implications of industry regulations,
  - PCI DSS
  - HIPAA
  - Data Privacy Frameworks (e.g., GDPR, CCPA)

APPLICATION SECURITY

- Analyze the Software Operations process for limitations that drive increased security risk and vulnerabilities
- Identify potential likelihood of an existing or future breach due to weaknesses in the application architecture
- Work with partners to identify known vulnerabilities in third party components utilized by the application

OPERATIONAL TECHNOLOGY

- Review and assess software applications and devices that directly control physical operations
- Examine and confirm OT system are in separate network
- Confirm controls are applied to relevant data sources

SECURITY ORGANIZATION & SPEND

- Identify security spend
- Review organization's cyber risk profile
- Design new entity's security organization for carve-outs/merger integration

Polling Question 1

What is the primary purpose of cybersecurity due diligence in an M&A or investment context?

(a) To identify potential cybersecurity risks and vulnerabilities

(b) To maximize the purchase price

(c) To streamline the deal process

Key cyber controls to evaluate and consider

The following cybersecurity controls can help reduce the likelihood and impact of an incident and are a key focus of cyber programs

- **Off-network Backups**
- **Multi-Factor Authentication (MFA)**
- **Email Platform Hardening**
- **Disaster Recovery, Business Continuity, & Incident Response Planning**
- **System Management, Hardening, & Patching**
- **Endpoint/Managed Detection and Response (EDR/MDR) Solution**
- **Security Information and Event Management (SIEM)**
- **Managed Security Services Provider (MSSP)**
- **Cybersecurity Insurance**
- **End User Security Awareness Training**
- **Privileged Account Management**
- **Penetration Testing & Vulnerability Scanning**

Cyber “non-negotiable”

Understanding a target’s disposition in the following cybersecurity controls can help reduce the likelihood and impact of an incident and should be a key focus of cyber programs

Off-network Backups
44% off-network backups;
7% protected & tested

System Management, Hardening, & Patching
43% full asset coverage;
42% established patch management program

Cybersecurity Insurance
95% have a policy

Multi-Factor Authentication (MFA)
80% at least one use case;
4% full MFA coverage

Endpoint/Managed Detection and Response (EDR/MDR) Solution
36% environment-wide coverage

End User Security Awareness Training
65% training;
50% phishing simulations

Email Platform Hardening
7% fully hardened tenants

Security Information and Event Management (SIEM)
18% implemented

Privileged Account Management
10% leveraged

Disaster Recovery, Business Continuity, & Incident Response Planning
3% documented & tested DR plan;
19% documented IR plan & runbooks;
14% conduct at least annual tabletop exercises

Managed Security Services Provider (MSSP)
35% leveraged

Penetration Testing & Vulnerability Scanning
21% both;
41% vuln scanning;
34% pen testing

**Solution implementation data and percentages were obtained from West Monroe’s Intellio Insights™ platform.*

Gaps in the below areas have resulted in lower cybersecurity resiliency and increased likelihood of business-impacting outages, and can also lead to loss of cybersecurity insurance or increases in premiums

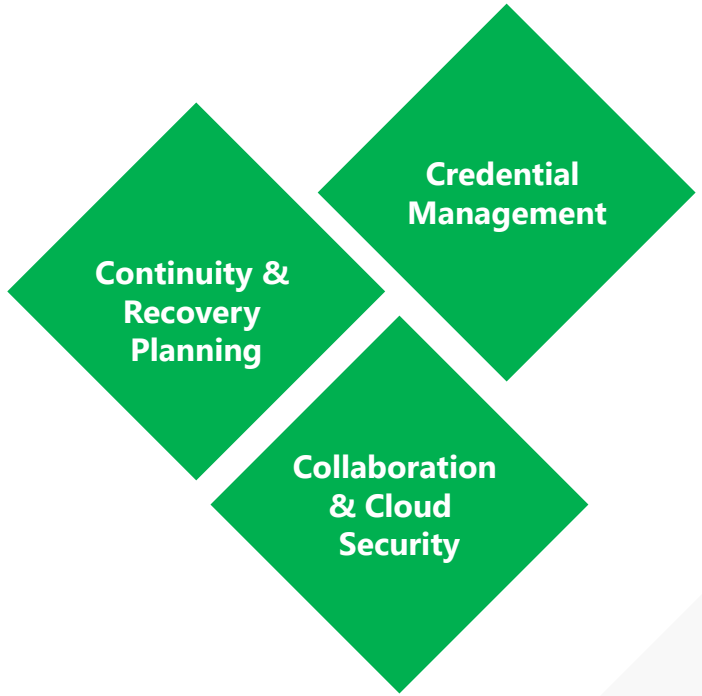
LOSS OF COVERAGE

- Multi-Factory Authentication (MFA)
- Managed Detection & Response (MDR)
- IR Plan Development & Testing
- Security Awareness & Training
- Secure Backups & Recovery
- Endpoint Encryption

PREMIUM INCREASES

- Privileged Access Management (PAM)
- Privileged Account Separation
- Email Security & Hardening
- Detection Capabilities (SIEM)
- 24/7 SOC Monitoring
- Penetration Testing
- Cloud Security
- BC/DR Design and Validation

POTENTIAL REMEDIATION ACTIVITIES



Polling Question 2

How can the estimated cost of remediating cybersecurity issues impact the due diligence process?

(a) It won't; cost is irrelevant

(b) It can affect the deal's valuation and terms

(c) It's only a minor consideration

While many companies leverage multi-factor authentication (MFA) for some use cases, there are additional use cases to which MFA should be expanded

EMAIL

REMOTE ACCESS

KEY BUSINESS APPLICATIONS

ADMINISTRATIVE FUNCTIONS

Approximately 80% of the companies we've evaluated/diligenced in the last two years have multi-factor authentication enabled for at least one of the above use cases, with the majority focused on email.

Expanding MFA usage to additional use cases was recommended at approximately 90% of companies.

Across due diligence and assessment engagements, West Monroe recommended enhancing backups at 80% of companies; common traits of backup implementations that allow organizations to recover quickly from a worst-case disaster scenario are highlighted below

PROTECT CREDENTIALS

Use a separate, non-synchronized credential set to access and manage backups

SYSTEM OBSERVABILITY

Monitor for new workloads, configuration changes, and job status. Act and follow-up on resulting operations tasks

SEGMENT STORAGE

Data is written to storage that cannot be easily accessed by malicious processes over the network

PROTECT CONFIGURATIONS

Ensure configurations are escrowed so that if backup infrastructure is lost it can be rebuilt quickly

VERIFY RECOVERY TIMES

Retrieval from offline repositories can be accomplished within defined RTO objectives

TEST RECOVERY

Beyond simple file level restores, full system and application tests are performed to validate functionality and timing

VERIFY FREQUENCY

Backups are taken frequently enough and held long enough to meet recovery point objectives

WM often finds email environments are not fully hardened, which increases the likelihood of business email compromise that can lead to a cybersecurity incident a data breach or ransomware attack

Account & Authentication

- Reduce number of administrators Remove administrative rights from standard users
- Enforce MFA for all accounts
- Block legacy protocols

Application Permissions

- Configure third party applications to require administrator approval
- Review application lists

Auditing

- Review audit logs on a set basis
- Configure alerting and monitoring
- Export email logs to a SIEM

Mobile Application / Device Management

- Require a PIN and encryption
- Containerize and protect mobile application data
- Block unmanaged devices and applications

E-mail Platform

- Configure SPF records
- Configure DKIM and DMARC
- Implement controls around spam filtering

Data Loss Prevention (DLP)

- Disable automatic external e-mail forwarding
- Configure DLP policies
- Disable external calendar sharing

Polling Question 3

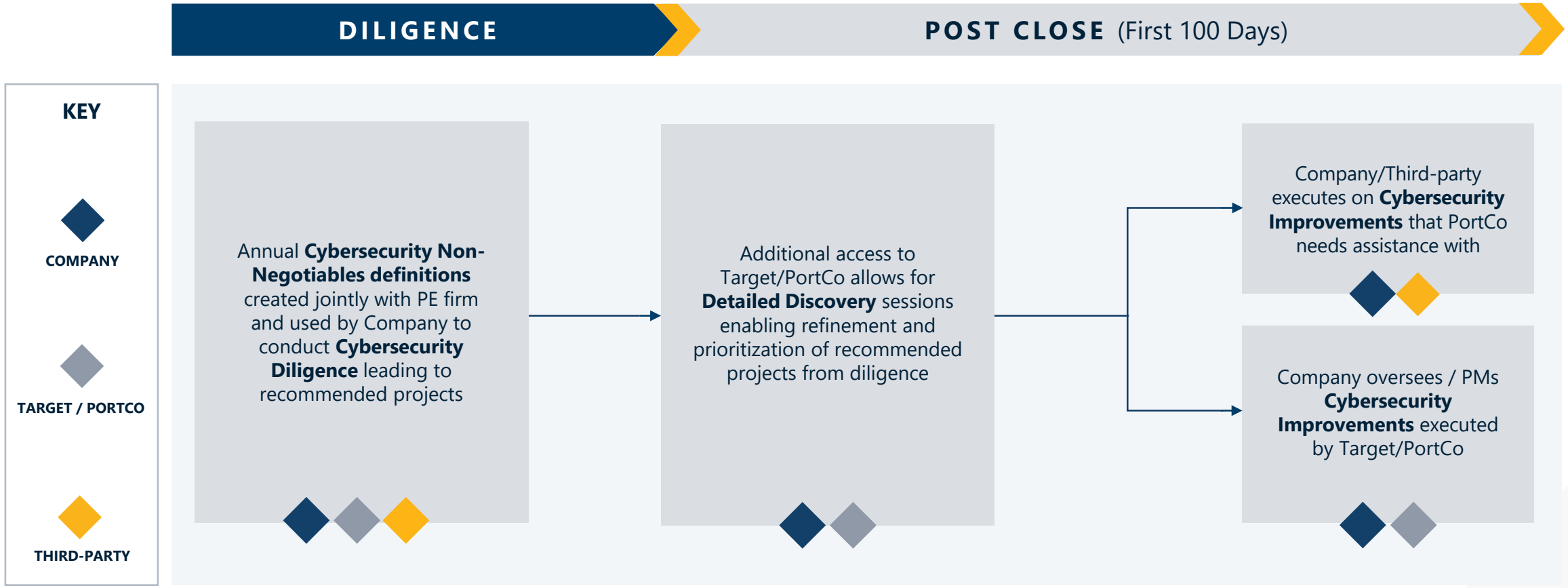
Which of the following is a key component of assessing cybersecurity risk during due diligence?

(a) Believing the target company's claims

(b) Relying solely on external audits

(c) Independent evaluation

Based on a jointly defined set of cybersecurity non-negotiables, an organization should prioritize understanding a company's cyber posture against those as part of diligence and then work to rapidly remediate as needed post close



Thank you.

Questions?

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!

The Institute of Internal Auditors Chicago

ISACA Chicago Chapter