

# Protecting Private Equity Portfolio Companies:

Using Data-Driven Insight to Mitigate Cyber Risk

### **Presenters**



Simon Eyre



Rebecca Thomas
Head of Account Management



**Greg Masino**Cybersecurity Advisor

# Cyber threat factors

# Factors that increase the likelihood of a cyber attack:

- 1. A public announcement of a transaction
- One PortCo falling prey to a successful cyber attack.

#### Factors that increase the impact of a cyber attack:

- Lack of cyber resilience at the PortCo.
- 2. Unknown cyber standards across the Portfolio.

#### The A Register

# EquiLend back in the saddle as ransom payment rumors swirl

Still no word on how the intruders broke in or the full extent of any possible data compromise

Connor Jones

Tue 6 Feb 2024 // 15:45 UTC

Global securities finance tech company EquiLend's systems are now back online after announcing a disruptive ransomware attack nearly two weeks ago.

# Impact of a successful attack

#### A successful cyber attack on a PortCo:

- 1. Negatively impacts the enterprise value.
- 2. Puts the entire portfolio at greater risk of being targeted by a cyber attacker.
- 3. Results in a problematic exit transaction.

#### What happens after a successful cyber attack:

- Ransom of intellectual property.
- 2. Erosion of trust among investors and other important stakeholders.
- 3. Increased cybersecurity insurance premiums.
- 4. Damaged reputation, lawsuits, regulatory fines, etc.

# Common Types of Successful Cyber Attacks

# **Business Email Compromise** (BEC)

- Low Barrier to Entry
- High Potential Financial Gain
- Lack of Advanced Security
   Measures
- Social Engineering
- Eagle Mountain City,
   Utah, sends \$1.13 million to
   vendor impersonator

#### Ransomware

- Anonymous Payment Methods
- Reputation Damage and Legal Consequences
- High Potential Financial Gain
- Social Engineering
- Time Sensitivity
- Ransomware group Lapsus\$ leaks password hashes for Nvidia employees

#### **Supply Chain Attacks**

- Difficulty in Detection
- High-Value Targets
- Limited Visibility and Control
- Sophisticated AttackTechniques
- MOVEit: The attack affected over 130 organizations worldwide



# Portfolio Highest Risks

- Multifactor Authentication for SaaS applications
- Personal Computers
- Regular Cybersecurity Training for Employees
- Mobile Device Management
- Keep Software and Systems Up to Date
- End of Life Hardware and Software
- Regularly Backup Data and Test Data Recovery Process
- Local Admin Rights
- Conduct Regular Security Audits & Assessments

# Challenges that we hear from PE clients

Challenge 1	IT Burden
Challenge 2	Cost
Challenge 3	Convenience
Challenge 4	Deal Team Support

# What should PE firms be doing?



Action item #1 – Assess cybersecurity as part of diligence during acquisitions.



Action item #2 – Prioritization and standardization of portfolio's cyber program.



**Action item #3** – Review of portfolios' cyber program roadmap.



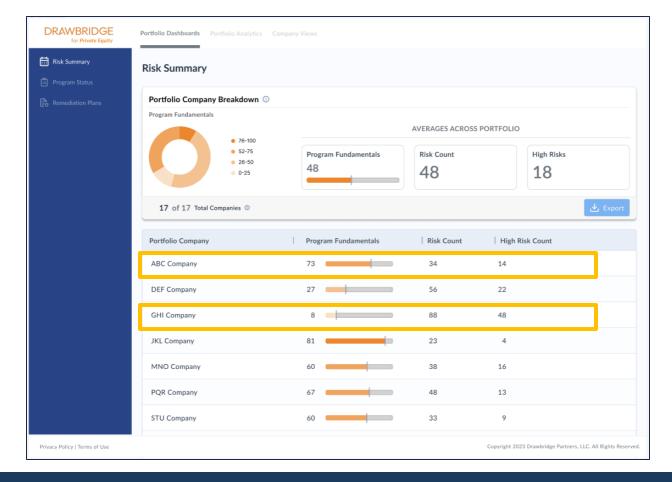
# How can Drawbridge help?

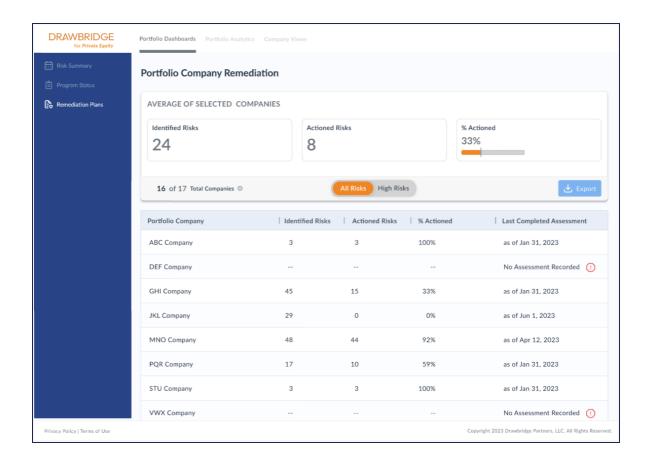
#### Phase 1

- Cyber Risk Assessment
- Cloud Assessments

#### Phase 2

- User Training & Awareness
- Vulnerability Scanning
- Penetration Testing
- Incident Response Tabletop Exercise





#### DRAWBRIDGE

# THANK YOU!

- +1 561-593-1600
- info@drawbridgeco.com | marketing@drawbridgeco.com | drawbridgeco.com
- 3300 PGA Boulevard, Suite 570 Palm Beach Gardens, FL 33410