Private Equity: Assessing Cybersecurity Across the Portfolio

December 12, 2018
Today’s speakers

Chris Wilkinson, Principal
Crowe LLP
Christopher.wilkinson@crowe.com
Cell: 219.308.8980

Kiel Murray, Senior Manager
Crowe LLP
kiel.murray@crowe.com
Cell: 814.450.2800

John Kurkowski, Partner
Crowe LLP
john.kurkowski@crowe.com
Cell: 312.560.1257
Today’s discussion goals

- Welcome and introductions
- Think like an attacker!
- Cybersecurity primer
- Cybersecurity assessments
- Phase one: Portfolio company prioritization
- Phase two: Assessment of risk
- Questions and closing remarks
Think like an attacker!

**Password policy for company X:**
- **Length:** 8 characters
- **Complexity required:** Three of the four (A, a, 1, !)
- **Lockout:** 3 Attempts
- **Lockout duration:** Forever

**QUESTION:** Given the above password complexity is enabled on the system, what be would *your first guess* for user account passwords?
Cybersecurity primer
Threat actors

Who's behind the breaches?

- 73% perpetrated by outsiders
- 28% involved internal actors
- 2% involved partners
- 2% featured multiple parties
- 50% of breaches were carried out by organized criminal groups
- 12% of breaches involved actors identified as nation-state or state-affiliated

Top external actor varieties in breaches

- Organized crime: 681
- Unaffiliated: 215
- State-affiliated: 138
- Nation-state: 21
- Former employee: 15
- Other: 9
- Acquaintance: 7
- Activist: 6
- Competitor: 4
- Customer: 1

Source: 2018 Verizon Data Breach Investigations Report
Who is targeted?

Who are the victims?

- 24% of breaches affected financial organizations.
- 15% of breaches involved healthcare organizations.
- 12% Public sector entities were the third most prevalent breach victim at 12%.
- 15% Retail and Accommodation combined to account for 15% of breaches.

What else is common?

- 66% of malware was installed via malicious email attachments.
- 73% of breaches were financially motivated.
- 21% of breaches were related to espionage.
- 27% of breaches were discovered by third parties.
Prevention, detection, and response

It’s not a matter of ‘if’, it’s a matter of ‘when’

Three-phased strategy:
• Prevention
• Detection
• Response

To be able detect attacks that were not able to be prevented and to be able to limit damage by responding swiftly
Cybersecurity universe

Data Protection
Physical Security
Logical Security
Logging and Monitoring
IT Operations
Business Continuity Management
Third Party Risk Management
Employee Management
Security Configuration Management
Security Change Management
Secure SDLC
Compliance
Threat & Vulnerability Management
# Cybersecurity Risk and Control Framework

## Cybersecurity Domains

### Policies and Procedures
- Information Security Program
- Standard Operating Procedures
- Administrative Standards

### Roles and Responsibilities
- Organizational Structure
- Security Responsibilities

### Oversight and Strategy

### IT Risk Management
- IT Risk Definition
- Risk Appetite / Tolerance
- Risk Assessment
- Risk Monitoring

### Logical Security
- Authentication
- Access Management (User Requests and Terminations)
- User Access Reviews
- Segregation of Duties

### Threat and Vulnerability Management
- Anti-Virus Standards
- Vulnerability Management Programs
- Patch Management
- Incident Response

### Data Protection
- Data Classification
- Data Inventory
- Encryption
- Data Destruction

### Data Protection
- Data Classification
- Data Inventory
- Encryption
- Data Destruction

### Business Continuity Management
- Business Impact Assessment
- Contingency Plans
- Critical IT Systems Redundancy
- Disaster Planning
- Backup Processes

### Third Party Risk Management
- Data Sharing Inventory
- Security Review - Vendor Selection
- Security Review - Ongoing
- Third Party Network Access
- Contracts

### Physical Security
- Documentation Storage and Security
- Clean Desk Policy
- Data Center Physical Security

### Log Logging and Monitoring
- Application / Database
- Server
- Network / Wireless Log Aggregation
- SIEM

### Security Configuration Management
- Standard Build Procedures
- Configuration Certification

### Security Change Management
- Change Management
- System Integration

### Secure Development
- Secure Design
- Secure Coding Practices
- Secure Development
- Security Testing

### Employee Management
- Security Training
- Employee Policies and Standards

### IT Compliance
- FFIEC Cybersecurity Assessment Tool
- HIPAA Security and Privacy
- PCI
- NAIC Model Audit Rule
Cybersecurity assessments
Phase one: Portfolio company prioritization
Risk factors to consider

- Industry and geography
- Types of data (PCI, HIPAA, IP, Employee, etc.)
- Volume of sensitive data
- Sharing of data with third parties/vendors
- IT and InfoSec team characteristics
- Incidents experienced
- Past assessments performed
## Portfolio company – cyber-risk profiling

- Cyber-Risk profile built for each portfolio company based on **customized survey** of 10-20 questions/criteria (sample below)
- Overall **risk score calculated** and companies are tiered based on survey results
- **Cyber assessment prescription** and schedule built for each tier of companies
- Survey can be incorporated into **due diligence** work for potential Cyber risk of future portcos

<table>
<thead>
<tr>
<th>Portfolio Company</th>
<th>Industry</th>
<th>Cyber-Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORTCO1</td>
<td>Retail</td>
<td>87</td>
</tr>
<tr>
<td>PORTCO2</td>
<td>Healthcare</td>
<td>65</td>
</tr>
<tr>
<td>PORTCO3</td>
<td>Education</td>
<td>41</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Company name</th>
<th>Industry</th>
<th>Cyber-Risk Profile</th>
<th>What sensitive information do you store, transmit, or process?</th>
<th>How many 3rd parties do you share data with?</th>
<th>IT function in-house?</th>
<th>How many employees do you have?</th>
<th>How many IT employees do you have?</th>
<th>People dedicated to information security?</th>
<th>Security incidents in the last two years?</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORTCO1</td>
<td>Retail</td>
<td>✓</td>
<td>Customer Credit Card Information (PCI); Trade secrets, other internal information</td>
<td>11-20</td>
<td>Outsourced</td>
<td>1,001-5,000</td>
<td>&lt;10</td>
<td>No formal security function exists</td>
<td>1-2</td>
</tr>
<tr>
<td>PORTCO2</td>
<td>Healthcare</td>
<td>✓</td>
<td>Health Records (HIPAA); Social security numbers,</td>
<td>50-100</td>
<td>In-house</td>
<td>5K-10K</td>
<td>51-150</td>
<td>Outsourced security function</td>
<td>3-5</td>
</tr>
</tbody>
</table>
Phase two: Assessment of risk
Factors to consider

Confidentiality

Availability

Integrity

Assess

Remediate

Maintain
Cybersecurity health check

Best for situations where:
- Companies are just getting started addressing cybersecurity
- Policies and procedures have been developed but not reviewed
- Limited testing with tools to get high level data on areas of improvement
- Organization wants to determine the maturity of cybersecurity domains at a high level

Approach:
- Focus on governance: approximately 25 hours of effort
- Cybersecurity policy and procedures review
- Interview with key IT resources
- Limited tool scanning

Limitations:
- Review of control design only
- Limited insight to vulnerabilities
Penetration testing

Best for situations where:
- Organizations have previously performed a cybersecurity assessment and addressed gaps
- Company is comfortable with current cyber policies and procedures
- Real-world hacking exercise of all systems, answers “What could an attacker actually do?”
- Other areas such as phishing and wireless testing can be added to scope

Approach:
- Depending on scope of systems: 60-80 hours of effort is typical
- Comprehensive testing of all internal and Internet facing systems
- Determine organizations ability to detect, contain and respond to activity

Limitations:
- Review of control design is not performed, only operating effectiveness
- Policies and procedures typically not covered
Hybrid assessment

Best for situations where:
- Organizations have established at least an initial cybersecurity program
- Policies and procedures have not been reviewed
- Penetration testing has not been performed

Approach:
- Focus on strategic and tactical areas: approximately 40 hours of effort
- Limited penetration testing to provide insight to high risk areas
- Analysis of maturity across cybersecurity domains
- Review of policies and procedures
- Interviews with key IT resources

Limitations:
- Lack of comprehensive testing, focus on high risk areas
- Limited insight to vulnerabilities
## Cybersecurity assessments – areas of coverage

<table>
<thead>
<tr>
<th>Scope – area of coverage</th>
<th>Health check</th>
<th>Hybrid assessment</th>
<th>Penetration testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber-Risk Profile Assessment</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cyber-Threat Analysis</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sensitive Data Classification</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Policies and Procedures Review</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Interview Key IT Resources</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Scanning</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Ethical Hacking (Servers)</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Ethical Hacking (Workstations)</td>
<td>Yes*</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Detective Control Capabilities</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Vulnerability Impact Analysis</td>
<td>Yes*</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Threat Analysis Reporting</td>
<td>Yes*</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Follow Up Testing</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Cybersecurity assessments: Takeaways

Not all companies carry the same amount of risk!

- Perform an initial risk assessment to focus the efforts if resource or budget constraints are in place
- All companies (that have digital assets) do carry some risk
  - Sensitive data in a variable, not a constant

Assessment results: How to interpret the gaps?

- All companies should not be graded on the same test
- Tie vulnerabilities (gaps) back to top threats (Ransomware, malicious employee, etc.)
- Focus on the impact to the business – set flags for penetration testing
- Follow up in six months to ensure progress
- Many common gaps can be addressed at the PEG level
  - Policies and procedures, governance, toolsets, etc.
Questions?

Chris Wilkinson
Christopher.Wilkinson@crowe.com
Cell: 219.308.8980

Kiel Murray
Kiel.Murray@crowe.com
Cell: 814.450.2800

John Kurkowski
John.Kurkowski@crowe.com
Cell: 312.560.1257