RISK strategies

PRIVATE EQUITY & VENTURE CAPITAL

Cyber: Private Equity's New Priority

The Cyber insurance market is at an inflection point where significant losses, concern surrounding systemic risk, and increased regulatory scrutiny are driving up Cyber insurance premiums and retentions at a fast pace. More than ever, private equity firms need to consider the cybersecurity of their firm and their portfolio as a top priority.

Private equity firms store large amounts of sensitive first and third-party data, have access to large quantities of capital and have frequent online financial transactions, all which make them a prime target for cyberattacks. In February 2022, the SEC proposed new rules under the Investment Adviser Act of 1940 to protect fund investors, which will require registered Investment Advisers and registered investment companies (registered funds) to implement cybersecurity risk management programs and new incident reporting guidelines. If adopted, advisers and registered funds will be required to 1) disclose detailed information about their cybersecurity incidents to current and prospective clients and shareholders; 2) notify the SEC within 48 hours of any significant cybersecurity incidents; and 3) implement cybersecurity policies and procedures that are reasonably designed to address their cybersecurity risks.[1] If the new rules are adopted, private equity firms will have increased compliance obligations and new regulatory risks due to possible cybersecurity exam deficiencies and enforcement actions.

Often, portfolio companies' poor cybersecurity controls can impact a private equity firm's return on investment (ROI). Cyberattacks have immediate operational and financial costs that can erode the value of a company. Consequences of a successful attack include revenue loss, brand reputation damage, loss of intellectual property, legal fees and other direct costs incurred to mitigate an attack. Private equity firms can avoid erosion of their ROI by investing in the cybersecurity of their portfolio companies and transferring direct financial risk to a dedicated cyber insurance program.

Top 10 most common initial attack vectors[2]:

1. Compromised Credentials
2. Phishing
3. Cloud Misconfiguration
4. Vulnerability in Third-Party Software
5. Physical Security Compromise
6. Malicious Insider/Rogue Employee
7. Accidental Data Loss/Lost Device
8. System Error
9. Business Email Compromise
10. Social Engineering

We recommend private equity firms include a thorough review of prospective portfolio investments' cybersecurity controls in their due diligence process pre-closing. Diligence steps can include:

1. discuss current controls in place with the company's CIO/CTO and identify potential gaps;
2. review contractual agreements with clients and third-party vendors;
3. determine if the target is in compliance with regulatory requirements (HIPAA, GDPR, CCPA etc.); and
4. examine insurance policies, claims and losses.

Cyber insurance has become an integral part of any M&A transaction. When Representations & Warranties (R&W) insurance is being utilized with a transaction, R&W carriers are now requiring the purchase of a Cyber insurance policy at closing and stipulate this policy should extend coverage to wrongful acts committed prior to deal close. Prior acts coverage for the target company can be obtained either through the purchase of a new Cyber policy at closing with full prior acts, adding to a platform with existing cyber insurance with full prior acts, or through the purchase of a Cyber Runoff/Tail policy if the go-forward carrier will not provide the requisite prior acts. There are nuances to these insurance options and the availability of Cyber coverage will be determined based on the target company's industry, loss history, and existence of current Cyber coverage. Please contact Risk Strategies for consultation on M&A Diligence and review of these Cyber options for a prospective investment.

Cyber Insurance Market & Renewal Checklist

Cyberattacks have increased considerably from 2020 to 2021 in both frequency and severity. The number of encrypted threats and ransomware attacks more than doubled over that same period.[3] Individual companies experienced a 31% rise in attempted intrusions and successful attacks.[4] The average cost of a breach increased 10% to $4.24 million in 2021 while the average cost of a ransomware breach hit $4.62 million. The industries with the highest breach costs include:

- Healthcare
- Financial
- Pharmaceutical
- Technology
- Energy

The industry sectors that experienced more than a 50% increase in cost over the prior year include Media, Public Sector (Government, Utilities), Hospitality, and Retail.[5]

In response to the rising number of reported claims and increased costs, carriers are seeking significant increases in premium and/or retention. Cyber premiums are generally increasing by an average range of 50-200% depending on the industry, quality of security controls and loss history.

PRIVATE EQUITY & VENTURE CAPITAL

Cyber: Private Equity's New Priority

To help your organization prevent and manage cyber threats and prepare for your Cyber Liability renewal, below is a checklist of some frequently recommended IT security controls. Carriers are closely reviewing insurance applications to determine if these best practices are in place, which may impact your renewal.

Cyber Security Control	Required	Best Practice
Automated Virus Scanning	√	
Laptop and Mobile Devices Encryption	√	Only permit applications trusted by your organization to run on devices
Network Password Protection (including Laptop and Mobile Devices)	√	
Macros - Disable macros from automatically running	√	
Media/Internet Usage	Controls on the insertion or use of media which does not carry appropriate authentication	Filter web browsing traffic. Use DNA to deny access to known malicious domains. Use web-isolation and containment technology.
Multi-Factor Authentication for 1. all remote access to the Insured's network for employees and external third-party vendors and contractors 2. all corporate email 3. all cloud services 4. privileged accounts including domain administrators and system administrators	Enable two-factor authentication. If using Office 365 use Office 365 Advanced Threat Protection.	Have MFA implemented at least 90 days prior to insurance renewal
Remote Access	Do not expose Remote Desktop Protocol directly to the internet. Use Remote Desktop Gateway or secure behind an MFA enabled VPN.	
Routine infrastructure back-up and testing of data restoration from backups	Regular backups. Annual Testing of data restoration	Testing every 6 months and MFA required to access backup. Backups are encrypted. Backups are immutable. Disconnect back-ups from organization's network.
Conduct routine vulnerability scans, preferably by a third party vendor	Annual	2 to 3 times a year
Restrict User Rights to Necessary Access	√	

Cyber Security Control	Required	Best Practice
Use of Endpoint Protection Platform (EPP) and/or Endpoint Detection and Response (EDR)	EPP	EDR
Established Process for Timely Software Updates	Critical patches addressed within 30 days of release	Every 2 weeks
Segregate and replace end-of-life or end-of-support software.	√	
Segmentation of Operational Technology and Information Technology	√	
Use of Security Operations Center (SOC) or Managed Detection and Response (MDR)	√ – Dependent on Size of Organization	√ – Dependent on Size of Organization
Enforce best practices on Service Accounts (see recommended actions below)		√
Conduct Employee Privacy and Phishing Training	Annual	2 to 3 times a year
Ensure you have a Business Continuity or Disaster Recovery Plan in place	Annual Testing	2 to 3 times a year and engage in tabletop exercises to test the plan
Require dual authorization for Fund Transfer Request		Required for Social Engineering Coverage
Vendor/Supplier Account Change Confirmation Requested via Second Means		Required for Social Engineering Coverage
Established Process to Use FBI Financial Fraud Kill Chain		√

FAQ's Regarding Key Security Controls

Multi-Factor Authentication Include for Privileged Account Users (Administrator Accounts)

What is it?

Multi-factor authentication (MFA) verifies the user's identity using multiple independent methods. Examples of authentication factors are one-time passwords (OTPs), physical security token, mobile device authentication, and biometric verification such as a fingerprint scan or facial recognition.

Why is it important?

Traditional systems using just User ID and Password are easily compromised. Attackers have many different techniques to gain access to these systems: brute-force attacks, phishing, malware, plain text password storage, key logging, social engineering, etc. Password re-using and Administrator password sharing also make it more likely that an account will be compromised. MFA provides an additional layer of security on top of login credentials. This layered defense makes it more difficult for an unauthorized user to access the network or database.

How is it implemented?

We recommend you deploy MFA across the entire organization, including remote network access for employees and business partners. MFA should include all end users, including administrative and privileged users, cloud and on-premises applications, server logins and Virtual Private Network (VPN).

Make MFA user friendly to ease the burden of employees. Offer a range of authentications factors: text, email verification, PIN, and security tokens. Remember the user's browser so each use doesn't require MFA. Common MFA vendors include: Auth0; Duo; Okta; and OneLogin.

Endpoint Protection Products (EPP) and Endpoint Detection & Response Products (EDR)

What is it?

Endpoint Protection Products (EPPs) and Endpoint Detection & Response Products (EDRs) are vendor provided tools that provide security capabilities like anti-malware scanning and incident detection and response. Endpoints are any device that is physically an end point on networks such as servers, desktops, laptops, mobile phones, printers, etc.

EPPs prevent traditional threats like known ransomware and malware. These products test for malicious behavior of files, identify behavioral anomalies and restrict access to specific IP addresses, applications, and URLs.

EDRs detect and respond to threats. These tools have the ability to detect malicious activity, block security incidents at network endpoints to prevent attacks from spreading and allow for investigation of incidents by maintaining a storehouse of endpoint data.

Why is it important?

Implementing these solutions help your organization manage all fixed and mobile endpoint devices through a single system, simplifying management for IT staff and protecting against threats. EDRs provides real-time visibility to security teams, allowing them to react quickly to a threat and minimize the damage.

How is it implemented?

Vendors that provide both EPP and EDR offer the most comprehensive solution. We recommend looking for standard protection features including data encryption, application control, anti-virus, intrusion prevention and malware protection. EDR solutions should include risk assessments, current threat level, incident data search, threat hunting, malicious activity detection and containment. Common EPP and EDR vendors are Carbon Black Cloud; Crowdstrike; Sentinel One; and Windows Defender Endpoint.

Network Segmentation & Segregation

What is it?

Network Segmentation divides the computer network into small networks. Network Segregation uses different types of access controls to allow connection between hosts, services and the smaller networks.

Why is it important?

Segmentation and segregation help restrict how far an attack can spread within an organization's network. Network administrators are able to restrict unauthorized users from accessing particular subsystems. In addition, the division of the network reduces congestion and improves operational performance.

How is it implemented?

Create separate networks for each group of devices that hold sensitive data. Control access in-between your segmented networks using gateways. Use a demilitarized zone (DMZ), a semi-trusted network that your organization controls, in between the internet and your networks. Management and data interfaces should be separated either physically or virtually. Management interfaces that are used for carrying out privileged and administrative functions should be accessible from a separated network only open to select administrators. Design access controls to separate your networks. Gateways should restrict access to only the network devices' required ports and protocols. Connection should be closed to all other ports and protocols. Networks are operating on an allowed list instead of a blocked list.

Most insurers require Operational Technology (OT) to be segmented from Information Technology. Best practices include segmented OT from the internet, requiring MFA, and separate user accounts for each employee. Common Segmentation vendors include: AlgoSec; Fortinet; Illumio; and Tufin.

Security Operation Center (SOC) or Managed Detection & Response (MDR) Service

What is it?

A Security Operation Center (SOC) is a centralized site where a cybersecurity team monitors, detects, analyzes and responds to cyber threats and incidents. SOC's may have operational hours that match the organization's business hours, but many insurers are looking for centers that are operational 24/7/365.

If a SOC is out of scope for an organization or insurers are looking for use of an external Managed Detection & Response Service, this is an outsourced cybersecurity service used to augment your organization's existing security controls.

Why is it important?

MDRs are a practical solution for organizations that prefer not to staff and train a fully functional cyber team. Using an MDR can help improve response time and effectiveness. MDRs can swiftly prioritize alerts, distinguishing benign events from true threats. They provide actionable advice on best practices for containment and remediation. MDRs handling the daily monitoring of cyber threats can free staff to work on more strategic projects.

How is it implemented?

If your organization is deciding to use an MDR, think about what services will complement your existing security capabilities. Is the MDR service available 24/7/365? What's the primary method of communication with your team? How knowledgeable is their staff and how do they stay current on recent tactics directed at organizations such as yours? Common MDR vendors include: Crowdstrike; Cynet, Ragpid7; and SecurityHQ.

The above are just a few of the most frequently highlighted security controls Cyber underwriters are focused on in this challenging insurance market. Companies that can show stronger IT controls will benefit from lower premiums, lower retentions, and broader coverage terms. We encourage you to review your controls with your IT staff well in advance of your Cyber renewal, to ensure you have sufficient time to address any deficiencies and make improvements that can impact your ability to obtain Cyber insurance at competitive rates.

Risk Strategies will partner with you to guide you through the Cyber renewal process, pre-underwrite your risk to highlight areas underwriters will focus on, and provide you with a Cyber Security Assessment. This Assessment is based on your domain name(s) and is non-invasive to your network systems. It is for your own internal reference to aid in highlighting potential weaknesses from an IT perspective. The Assessment scans the internet for all vulnerabilities that a hacker might exploit, such as open ports, security flaws, exposed data, and passwords, and provides you with a scorecard and actionable recommendations to improve your Cyber security risk profile. As a specialty broker with expertise in the Cyber security arena, Risk Strategies takes a holistic approach to risk management by addressing clients' risks proactively from the pre-underwriting stage in order to best position your risk for your Cyber placement.

ENDNOTES

1. Debevoise & Plimpton "How Private Equity Firms Can Prepare for the SEC's Proposed Cybersecurity Rules" May 2022
2. IBM Security Cost of a Data Breach Report 2021
3. Sonicwall 2022 Cyber Threat Report
4. Accenture State of Cybersecurity Resilience 2021
5. IBM Security Cost of a Data Breach Report 2021

If you have questions regarding this article or your current coverage, please contact our Private Equity Practice Group:

Michael McFadden
Managing Partner
750 Third Avenue, Suite 150,
New York, NY, 10017
484-354-8508

Kevin Flasch
Managing Director,
Private Equity Practice
750 Third Avenue, Suite 150,
New York, NY, 10017
646-234-5846

Stephanie Needham
Senior Managing Director
160 Federal St, 4th floor,
Boston, MA, 02110
617-877-0691

Sara Wice
General Counsel
750 Third Avenue, Suite 150,
New York, NY, 10017
212-596-3452

Want to Learn More?

VISIT OUR KNOWLEDGE CENTER

https://www.risk-strategies.com/knowledge-center

ABOUT RISK STRATEGIES

Risk Strategies is a specialty national insurance brokerage and risk management firm offering comprehensive risk management advice and insurance and reinsurance placement for property & casualty, employee benefits, and private client services risks. With more than 30 specialty practices, Risk Strategies serves commercial companies, nonprofits, public entities, and individuals, and has access to all major insurance markets. Ranked among the top brokers in the country, Risk Strategies has over 100 offices including Boston, New York City, Chicago, Toronto, Montreal, Grand Cayman, Miami, Atlanta, Dallas,