nerej
CELEBRATING 55 YEARS

Real estate and cyber liability - by Spencer Macalaster

March 31, 2023 - Spotlights

Spencer Macalaster

The past 36 months have been unprecedented with respect to society, work environments and political dictates. Entire companies pivoted to remote work environments in a matter of days. The consequential strain on the IT infrastructure was also unprecedented. One consequence of this new paradigm was system vulnerabilities were exposed. Every day a new company is added to the list of systems affected by a massive data breach. Hackers responsible for these types of security breaches can hold a company ransom or worse destroy their reputational credit. In the wake of the Silicon Valley Bank and Signature Bank failures, we expect bad actors to take advantage of the events to intercept wire instructions as clients and other third parties work to reroute funds to alternative banking institutions. We would like to reiterate the need to be wary of requests to change / update payment account information for invoices or any other payments to be made by the company and encourage you to remind our clients and other valued partners of the same.

Real estate owners, developers, and asset managers are in the crosshairs of those bad actors looking to monetize on cyber vulnerabilities. Massachusetts requires companies to provide comprehensive data security to all personal information stored on a server. In addition, regulators in 47 states, the District of Columbia, Puerto Rico, and the Virgin Islands require that individuals (customers, employees, citizens, students, etc.) be notified in the event their data has been lost, stolen or compromised. The most recent data breaches introduce a new twist to a company's cyber liability exposure and potential for exposure to extortion and ransom.

Computer hacking, stolen laptops and fraud scams are the primary culprits leading to cyber liability events. Settlements can include monetary damages, credit monitoring services, hardware and software restoration, business interruption, reputational damages and ransomware payments. Companies can incur millions of dollars in expenses to secure compromised networks, assess damages, and notify customers.

Protection on any corporate database will never be 100% secure. As soon as security measures, such as firewalls, are developed the cyber thieves are creating ways to breach those security measures. With the shift to remote work, contactless services, and increased health/safety precautions corporate exposures expanded dramatically. Internet security protection is a continual process that cannot be solved entirely by technical means. There are many steps you can take to enhance your protection. Implement multi-factor authentication, don't respond to emails or phone calls requesting your personal information. Use unique usernames and strong passwords for any online account. Make sure you have the most up-to-date security software installed on your computers. Cyber threats are now recognized as one of the biggest threats to business and individuals and are a matter of national security.

Cyber-crime is highly lucrative and provides huge financial incentives to the criminals who can derive large payouts from the data stolen. According to the IBM the average cost of cyber event is $3.8 million. Every company should evaluate the exposure and look into cyber insurance as a financial backstop to their data security risk management. Traditional insurance products, including property, general liability and professional liability, do not address cyber risks. As with most special

types of risks, it takes a specialty insurance product to address the exposure. Cyber liability policies have been expanding in coverage to include privacy notification expenses, hardware restoration, business interruption expenses and ransom costs.

The bottom line is all companies are exposed to data security breaches. The financial consequences can be enormous, historically most companies relied almost exclusively on technological solutions to manage the risk. There is a growing awareness at many companies that data security should not be exclusively an IT issue, making cyber insurance coverage a standard part of a company's risk management strategies.

In addition to evaluating the cost and coverage available through your insurance broker, we recommend conducting your own "cyber hygiene" analysis to protect against threats of loss. Cyber hygiene is a set of practices for managing the most common and pervasive cybersecurity risks faced by companies today.

• Identify and prioritize key organizational services, products and assets;

• Evaluate and respond to a company's key services and products;

• Establish an incident response plan;

• Maintain a proactive and continuous educational and training program;

• Maintain continuous and updated security and monitoring;

• Implement controls to protect and recover data;

• Monitor and manage supplier and supply chain dependencies;

• Implement "MFA" (multi-factor authorization) throughout the organization;

• Perform continuous cyber threat and vulnerability monitoring.

Cyber exposures require an all hands on deck approach. Hardware, software, training, and insurance must work in a coordinated way to fully protect your company from significant financial loss and reputational harm.

Spencer Macalaster is the executive vice president of Risk Strategies Co., Boston, Mass.