Cyber Risks & Liabilities

Third Quarter 2021

Promoting Cybersecurity in the Expanding Digital Economy

At the initial onset of the COVID-19 pandemic, organizations across industry lines were forced to implement digital offerings in an effort to remain operational. This shift to predominantly remote activities—such as video chatting, online shopping, electronic payments and contactless deliveries, among others—changed the way consumers were able to receive goods and services.

Specifically, the pandemic largely accelerated the nation's already expanding digital economy. As a result, many consumers are expected to continue leveraging online options for the foreseeable future—even as COVID-19 restrictions are lifted and organizations reopen their doors to the public. With this in mind, it's important for your organization to consider permanently integrating remote capabilities within your current products or services (if you haven't already).

Nevertheless, introducing online offerings comes with further cybersecurity considerations. Without proper precautions in place, implementing digital operations could make your organization increasingly vulnerable to cybercriminals—potentially resulting in costly attacks, devastating interruptions and reputational damages.

What's worse, cybercriminals are only becoming more sophisticated within this growing digital economy, thus making protective measures all the more vital. As such, your organization should make these cybersecurity adjustments alongside any remote offerings:

- **Conduct a cyber risk assessment.** First, perform a risk assessment to analyze the cyber exposures that could accompany your digital operations.
- **Establish workplace policies and procedures.** Use the risk assessment to develop policies and procedures that can help limit your organization's cyber exposures. This may include further employee training, extra authentication measures, additional data backup protocols and new security software.
- **Ensure compliance.** Review your organization's digital operations to make sure they are compliant with any applicable regulations—such as the Payment Card Industry Data Security Standard.
- **Create a cyber incident response plan.** Be sure to develop a response plan that will help your organization remain operational and minimize potential damages in the event of a cyberattack.
- **Secure appropriate coverage.** Lastly, consult a trusted insurance professional to help determine whether your organization needs additional coverage to protect against cyber exposures.

For more insurance solutions, contact us today.

Provided by Evergreen Insurance

EVERGREEN INSURANCE

Key Benefits of Penetration Testing

Penetration testing consists of an IT professional mimicking the actions of a cybercriminal to determine whether an organization's workplace technology possesses any vulnerabilities and can withstand their attack efforts.

This type of testing can offer numerous advantages to your organization, including:

- **Improved cybersecurity evaluations**—By simulating realistic cyberattack situations, penetration testing can help your organization more accurately evaluate its varying security strengths and weaknesses—as well as reveal the true costs and of any security concerns.
- **Greater detection of potential vulnerabilities**—If any of your workplace technology or other cybersecurity protocols fail during a penetration test, you will have a clearer picture of where your organization is most vulnerable. You can then use this information to rectify any security gaps or invest further in cyber initiatives.
- **Increased compliance capabilities**—In some sectors, organizations are legally required to engage in penetration testing. As such, conducting these tests may help your organization remain compliant and uphold industry-specific expectations.
- **Bolstered cybersecurity awareness**—Mimicking real-life cyberattack circumstances will highlight the value of having effective prevention measures in place for your employees, thus encouraging them to prioritize workplace cybersecurity protocols.

For more risk management resources, contact us today.

Preventing Supply Chain Cyber Exposures

In late 2020, the U.S. government revealed that Russian hackers had orchestrated a supply chain cyberattack earlier in the year in an effort to compromise several federal agencies and organizations. The hackers initially infiltrated the network monitoring platform of SolarWinds—a technology company—via malware before using that platform to gain access to sensitive data and emails from a range of government departments and private organizations.

The attack—which has been dubbed as one of the largest and most sophisticated breaches the world has ever seen—is estimated to have impacted over 18,000 of SolarWinds' customers and incurred as much as $90 million in total losses. The fallout from this large-scale attack has motivated many businesses to take a closer look at potential security risks stemming from their supply chains and make necessary adjustments to ensure cyber resiliency.

The first step in mitigating your organization's supply chain exposures is to understand where these risks come from. Such exposures can stem from a variety of parties and practices, such as:

- Third-party services or vendors with access to information systems
- Poor cybersecurity practices by suppliers
- Compromised organizational software or hardware
- Software security vulnerabilities in supply chain management or among third-party vendors
- Inadequate third-party data storage measures

While it's not possible to totally eliminate supply chain risks, there are several steps your organization can take to help reduce supply chain exposures and prevent costly attacks. Be sure to implement these precautions:

- **Incorporate cyber risk management into vendor contracts.** This can include requiring vendors to obtain cyber insurance, having them notify your organization after a cyber incident and establishing clear expectations regarding the destruction of data following the termination of your contracts.
- **Minimize access that third parties have to your organization's data.** Once a vendor or supplier has been chosen, work with them to address vulnerabilities and cybersecurity gaps.
- **Monitor suppliers' compliance with supply chain risk management procedures.** Consider adopting a "one strike and you're out" policy with suppliers that experience cyber incidents or fail to meet compliance guidelines.

For additional loss control guidance, contact us today.