CyberTalk.org

A CISO'S GUIDE TO PREVENTING DOWNSTREAM EFFECTS (AND LITIGATION) AFTER A BREACH

Sponsored by Cyber Talk

Introduction

How many third-parties does your organization work with? Seventy-one percent of organizations state that their third-party network includes more businesses than it did three years ago.

In the next three years, the same percentage of organizations expect that their third-party partnerships will expand even further. Third-party partnerships are valuable, multi-faceted tools until a security breach occurs. At that point, the downstream effects of a breach can lead to contractual obligation failures and litigation.[1]

60% of organizations work with more than 1,000 vendors

Ensuing breach litigation can be extremely intense and can impair businesses; rupturing business relationships, tarnishing reputations, and exhausting financial resources, among engendering other negative impacts. In some cases, breach litigation is a business extinction-level event.

In this cyber security whitepaper, we'll address key ways to reduce downstream liability issues in the event of a breach, with an emphasis on how to prevent legal battles. After reading this whitepaper, if your business experiences an attack that affects your third-party contacts, you will be in a stronger position to refute any litigation that may arise.

Cascading Effects

Downstream cyber risk, incidents and liability are particularly concerning for entities and industries that maintain complex interdependencies. For example, within the automotive industry, a cyber attack on an electronics systems supplier could stymie efforts to continue manufacturing vehicles in separately owned and operated plants.

What is downstream liability? Downstream liability refers to how a company's business partners, suppliers and clients are affected in the wake of a security failure.

[1] 7 Questions for a Vendor Risk Assessment, Sabrina Pagonotta, thirdpartytrust.com. https://www.thirdpartytrust.com/blog/vendor-risk-management-questions-assessment/

Possible real-world outcomes include significant economic losses for a series of companies, the erosion of trust between businesses, and exorbitantly high parts and vehicle prices for consumers, among other unwanted effects.

The Cost of Failure

The cost of failure is high. On average, incidents with downstream implications cost organizations roughly $432,000, but costs have been known to exceed $163 million. Over 80% of incidents with ripple effects involve financial damage payouts. Fifteen percent of 'ripple incidents' force defendants to pay roughly $8.3 million in response costs.[2] While some lawsuits are indeed settled prior to going to trial, they still impose distracting, needless theatrics and reputational damage.

> Over 80% of incidents with ripple effects involve financial payouts

Case Study

Recent cyber incidents highlight the challenges associated with preventing downstream effects.

In an outsized, notable example, the attack on Colonial Pipeline not only affected business partners, but it also temporarily disrupted the businesses that relied on its operations. Due to the loss of business income on account of the attack, small gas station owners filed a class-action lawsuit.

Another lawsuit filed against the company claims that consumers were harmed by increased fuel prices due to the pipeline shutdown. The claimants allege that the company failed to adhere to appropriate cyber security standards.[3]

This case study exemplifies the ease of unintentionally precipitating downstream effects, and the litigiousness of some downstream parties.

---

[2] Ripple Effects from a Cyber Incident Take a Year to Develop: Report, Samantha Schwartz, Cybersecuritydive.com, Sept. 27, 2021 https://www.cybersecuritydive.com/news/ripple-cyberattacks-supply-chain-third-party-cost/607220/#:~:text=It%20takes%20more%20than%20a,RiskRecon%20and%20the%20Cyentia%20Institute

[3] Lawsuits Allege Colonial Pipeline Had Inadequate Cybersecurity, Scott Ferguson, Bankinfosecurity.com, June 23, 2021 https://www.bankinfosecurity.com/lawsuits-allege-colonial-pipeline-had-inadequate-cybersecurity-a-16928

Mitigation Before Litigation

Mitigate potential negative externalities ahead of contending with extreme business situations, such as legal claims and expenditures. Invest in optimal levels of security prevention and precautions, as suggested by the following best practices:

1. CLASSIFY DATA AND MAP DATA FLOWS.

Data flow maps are commonly used in cyber security planning stages to identify the types of information that an organization needs to secure. The utility of a data flow map is that it will depict sensitive information based on origins, paths, exit points and storage locations. Further information can be diagramed, detailed and applied as information overlays, including who has access to data at various points and the type of access they require. Also known as Threat Modeling, this is key in understanding how to incorporate measures to prevent unauthorized access.

Mapping should include network infrastructure devices, servers, endpoints, protocols, firewalls, printers, CD/DVD burners, backup tape drives and endpoints where sensitive information can be added to portable media.

This task eventually reveals locations where security needs to be added and maintained, resulting in stronger protection of sensitive information.

2. IMPROVE VISIBILITY.

Many organizations aren't fully cognizant of their entire spread of business relationships, and a large portion lack insights into all of the dependencies that their direct connections have on other firms. While an organization may have policies around acceptable supplier, vendor, or client security, those groups may not retain the same types of policies, and may work with less secure organizations.

Connections and interconnectedness can prove surprising. It pays to improve visibility into downstream business ecosystem connections. Vendor risk assessment should include participation from the legal, privacy, security, and IT teams, as well as the business unit(s) for whom the vendor is being utilized.

3. TEST YOUR SECURITY TO PROVE THAT DATA IS SECURE.

Conduct regular, standardized security penetration testing and vulnerability assessments of internal and external networks, along with social engineering testing. Such tests can include simulated phishing emails and employee awareness tests. Document follow-up findings, along with mitigation or remediation strategies pertaining to any issues identified. Retain documented evidence that you test your security - preferably using an un-biased third-party - at least once per year.

4. DETAILED CLIENT CONTRACTS.

While the ubiquity of email means that written documentation is inherently available, it never hurts to ensure that the entirety of an organization's contracts spell out services provided in the event of a breach, along with liability limitations and other mutually beneficial legal protections. Documents should be reviewed by all relevant parties' legal, privacy, security, and IT-teams.

Often times, organizations informally administer cyber security assessments to vendors, partners and suppliers. While the document might literally have all of the boxes checked, in many instances, legal teams never create or review these documents, rendering them weak evidence in the event of litigation.

5. INSURANCE COVERAGE.

Third-party cyber liability insurance covers expenses associated with cyber attacks, data theft, and network data losses. In the event that a partner, supplier or client sues your organization, third-party cyber insurance may pay for legal expenses. These may include attorney's fees, court costs, and court-issued penalties. If your organization maintains an errors and omissions insurance (E&O) policy, third-party liability may or may not be included – be sure to check.

6. VENDOR LIFECYCLE MENTALITY.

A partner or supplier's ability to manage risk may evolve over time, and may be related to an organization's financial health, regulatory requirements, market conditions or other factors. Nonetheless, your organization retains a responsibility for monitoring the cyber health of partners and suppliers from on-boarding to off-boarding.

Seventy-five percent of enterprises only see ripple effects a year or more after an attack, meaning that the catalyst organization may face unexpected calls, emails and lawsuits long after an initial incident occurred.[4] Ensure that your organization retains detailed security documentation for extended lengths of time. Consider backing these up to off-site locations, should your organization suffer a breach.

[4] New Research Compares Multi-Party Data Breaches to Single Party Events, riskcrecon.com, Sept. 21, 2021 https://blog.riskrecon.com/new-research-compares-multi-party-data-breaches-to-single-party-events

Conclusion:

On account of technological and organizational complexity, managing the downstream effects of and liability for cyber fallout is becoming an increasingly large burden for organizations.

Although a perfectly secure cyber ecosystem would be the ideal, it does not exist. Following the guidance outlined above will empower organizations to protect third-parties, and themselves when it comes to breach prevention and incident liability.

For further expert insights concerning cyber security liability, please visit CyberTalk.org, or reach out to your local Check Point representative.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com