SOLUTION NOTE

IMPROVING CYBERSECURITY REPUTATION WHILE REDUCING CYBER INSURANCE COSTS

OVERVIEW

Recent ransomware and supply chain attacks have shown us that in an increasingly connected world, no organization or industry is safe from attack.

Even traditional industries such as oil and gas and infrastructure such as food processing plants can face significant disruption from cyber attacks. Increased reliance on digital devices and processes, accelerated adoption of cloud and SaaS services and the move to a hybrid workplace model mean one thing—increased exposure to cyber risk.

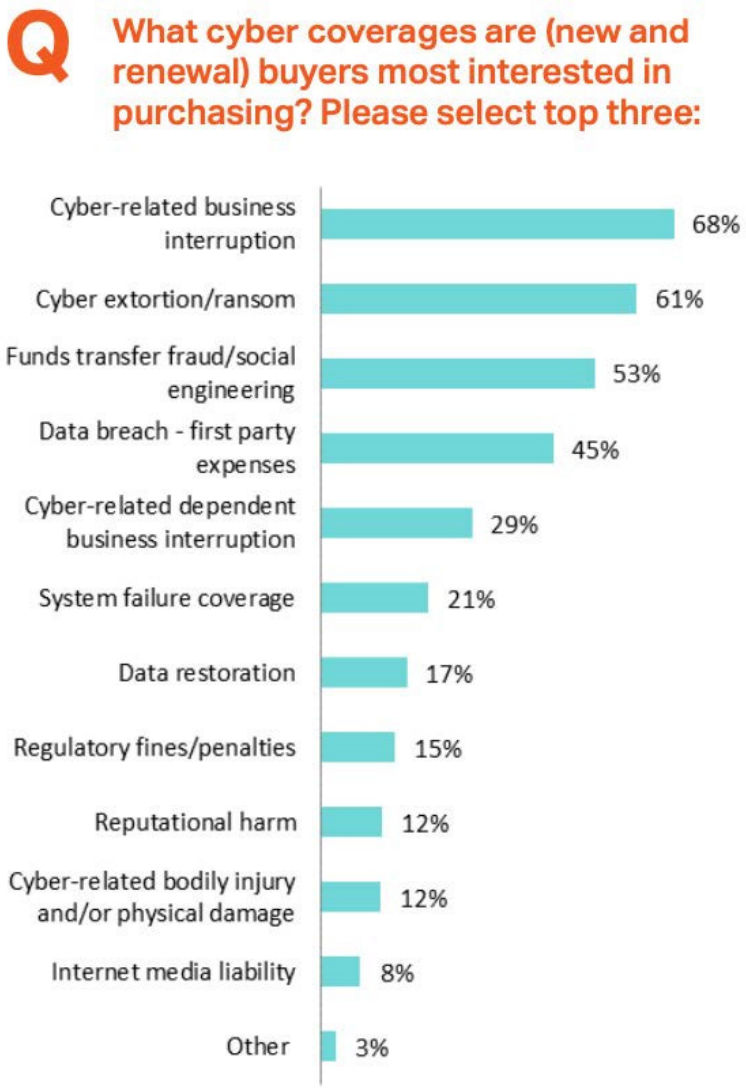
Persistence of supply chain attacks is forcing companies to take a hard look at their vendors and their vendors' security posture. One of the ways that organizations try to manage third-party risk is by looking at security scoring/ratings for those third-party companies. If a vendor has a poor security posture or cyber reputation, it can have repercussions on the organization itself, leading to lost deals, customers moving to competitors and ultimately negative effects on revenue. These trends are leading businesses to hedge cyber risk with insurance. The bottom line is, with the persistence of cyber attacks, organizations need to not only invest and improve their own cybersecurity posture but also manage third-party risk while considering options like cyber insurance.

CYBER INSURANCE INSIGHTS

The cyber insurance market will be worth $20.4 billion by 2025, up from $7.8 billion in 2020 (CAGR 21.2 percent), according to MarketsandMarkets. Cyber insurance premiums are increasing every year, driven by fast growth in ransomware claims, increasing security breaches and attacks resulting in huge losses. Cyber insurance can cost anywhere from the low hundreds of thousands to millions of dollars per year.

The ways insurance companies assess businesses have become more complicated in recent years, usually including one or more of the following measures:

- Audit of assets, applications, business processes and existing security processes
- A minimum requirements approach, based on whether the organization has implemented security measures such as use of multi-factor authorization
- Independent third-party audits and security scores
- Assessment of a business's capability to recover data in case of a ransomware attack



Cyber insurance buyers clearly are driven by media coverage of cyber attacks and first-hand experience with losses from IT security events.

Source: Cyber Insurance – The Market's View, Advisen / PartnerRe

Security Scoring

Insurance companies also use security scores to assess risk of applicants. The higher the security score for a company, the better its posture—meaning it is at a lower risk of a data breach. Security scoring companies use various measures and publicly observable data to determine a company's score and posture. A key element in this equation is the organization's Domain Name System (DNS) infrastructure. DNS plays a vital role when it comes to public data because it is in the pathway for all Internet communications. Implementing DNS security can improve the security score for a company, thereby improving its cyber reputation and potentially lowering insurance costs.

DNS SECURITY FOR IMPROVING SECURITY SCORES AND REDUCING CYBER INSURANCE COSTS

DNS security provides visibility, protection and security automation to improve a company's security posture.

Visibility: When implemented through today's most advanced solutions, DNS, DHCP and IP address management, together called DDI, can provide precise visibility across the entire distributed enterprise. Done right, DDI can help you identify all devices, workloads and users on your network and what they are doing at any given time. This visibility extends to cloud environments, remote branch locations and home offices, providing IT teams with a complete view of everything that is happening on the network. In addition, DDI data can help them to quickly triage and respond to incidents.

Protection everywhere: Using threat intelligence and AI/ML analytics-based threat detection on DNS servers, you can detect and block modern malware, including ransomware, data exfiltration, domain generation algorithms (DGAs) and more, throughout the distributed enterprise. You can protect not just your HQ/data centers but also your cloud workloads, IoT environments, remote offices and home offices using DNS layer security. It's a cost-effective and powerful first line of defense that can protect anything from an HVAC system to cloud workloads and everything in between.

Security automation: DNS security integrated with the broader security ecosystem can automate incident response when an IT security event does occur. For example, when an event is detected by the DNS security solution, a vulnerability scan can be triggered on the compromised device to check for any vulnerabilities. The event can be shared with SIEM/SOAR tools for further analysis. You can also automatically raise an IT ticket to get that device remediated. Thus, DNS security enables closed-loop threat response using integrations to automatically share events and network context with SecOps tools for faster remediation.

All these capabilities greatly improve an organization's cybersecurity posture, its brand reputation and its security score, while eventually lowering cyber insurance premiums.

CUSTOMER STORY: FRENCH ENERGY AND AUTOMATION SOLUTIONS COMPANY

This French company provides digital automation solutions for energy sustainability and efficiency.

Business Need: Portray strong security posture to business partners and customers.

Challenge: The company was paying high premiums for cyber insurance due to a poor security score. It had challenges with getting partners and customers to do business with.

Solution: The company deployed Infoblox DNS security, and within a few months its security score improved from an intermediate score of 670 to an advanced score of 800. No other technology was deployed during that score improvement period. Now the company has the best score of all 40 top French companies, and it also saved $1.2 million on cyber insurance fees over a three-year period because of its score improvement.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240206v1