BioSpectrum the business of Bio & Health Sciences

Third-party cyber risks: a blind spot for pharma industry

19 May 2021 | Views

When the vaccines are shipping globally, hackers use the weak links within the supply-chain units to further cripple the pharmaceutical industry

On the partly sunny, overcast day of June 27th, 2017, a mother of two reached her office in New Jersey, to read - "All networks and services are down. Do NOT turn on your computers. Remove all laptops from docking stations and keep them turned off. *No Exceptions*" - a handwritten sign in front of the glass doors greeted her. She proceeded to her desk to find her colleagues locked out of their systems, watching videos or playing candy crush on their cell phones. Every computer screen flashed a warning note in glowing letters: "Ooops, your important files are encrypted. We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment …." Three years since this incident that is now famous as the NotPetya ransomware attack, Merck is currently staring at a loss of at least $1.3 billion. A data breach costs an average of $5.20 million in this sector. Add $370,000 more if the breach happens through a third party. However, the impact goes beyond the financial repercussions in this sector -- when drug research, production, supply, or sale stalls, lives are at stake.

Has this industry learned from past errors?

Case in point, in September 2020, Gavi, Vaccine Alliance's Cold Chain Equipment Optimization Platform, received an email from Haier Biomedical - "the world's only complete cold chain provider" - requesting familiar quotations. In the email, there were regular-looking HTML attachments that asked the recipient to enter specific credentials. Unfortunately, this was a spear-phishing campaign sent to select executives in sales, procurement, information technology, and finance. According to IBM X-Force's evaluation, this attack, spanning over six countries, was to harvest credentials to gain future unauthorized access to corporate networks and sensitive information.

In search of the path of least resistance, cyber attackers have recently hit gold by targeting the vast (and expanding) network of third-party suppliers, contractors, and vendors. The supply chain of pharmaceutical companies is a treasure trove of intellectual property, PHI, sensitive research, and a lot more. According to The 2020 State of Cybersecurity Report, a closer look at the sources of cyberattacks reveals 40% of security breaches were indirect, as threat actors target the supply chain ecosystem as the weakest link. This statistic remains relatively constant across industries.

What is the solution?

While most pharmaceutical businesses have been cautious about their cybersecurity posture, they are still not exempt from being one of the most targeted sectors of all. Upping cyber risks originating from a third or nth party starts with mapping their respective digital footprint. For the entire digital footprint of a third-party, a non-intrusive, outside-in risk assessment should be performed including the following:

- **Email Security:** for DNS settings that identify and avoid incoming phishing/fraudulent emails
- **DNS Security:** for common unsecured configurations and vulnerabilities
- **Application Security:** for misconfigurations and vulnerabilities
- **Network Security:** for misconfigurations and vulnerabilities
- **System Security:** for insecure configuration
- **Breach Exposure:** for identification of inadvertent/intentional exposure of potentially sensitive information through a data breach of your vendor organization
- **Compromised Systems:** to detect systems and applications involved in malicious and/or unusual activity
- **Cyber Reputation:** to identify threats that may damage an organization's brand reputation and eventually affect its revenue

An organization has an average of 5800 third-party vendors. In order to streamline their cybersecurity assessments, a standard operating procedure should be defined. Organizations should categorize their vendors into three tiers based on their size and the level of critical data access available to them. In descending order of cyber risks, **Tier 1** vendors' cybersecurity should be assessed in real-time, followed by **Tier 2** vendors that should be assessed daily, and **Tier 3** vendors should undergo weekly assessments.

Assuming that basic security practices of vendor inventory and certification are in place, the next step in third-party risk management for enterprises is to use digital business risk quantification to their advantage. Such platforms continuously run automated scans to monitor the real-time cyber risk posture of all their business's critical third parties. To simplify the procedure, they can use a consistent risk metric such as their breach likelihood. Risks posed by an enterprise's third party 'web' are denoted as

1. **Critical**: Root-level compromise of servers or infrastructure devices with devastating consequences.
2. **High**: Elevated privileges and significant data loss, or downtime, indicating high priority remediation
3. **Medium**: Exploitation provides limited access but should not be ignored.
4. **Low**: Very little impact and low priority security alarms.
5. **Informational:** Security gaps that do not need immediate remediation.

The pharmaceutical industry is currently fighting a war with an invisible enemy. Cybercriminals are launching enterprise-level to nation-state espionage attacks leveraging both traditional and sophisticated means. Despite declaring a truce in the early phases of the pandemic, cyber attacks crippled this sector by targeting e-records through globally coordinated ransomware attacks. Later, during the vaccine research, CozyBear, Lazarus, APT29, Stone Panda, etc., have been notorious for targeting Asian pharmaceutical companies to pilfer Intellectual Property. Now, when the vaccines are shipping globally, hackers use the weak links within the supply-chain units to further cripple the pharmaceutical industry.

So with no signs of a slow down, businesses are undoubtedly leading efforts to shore up defenses to get ahead of the inevitable next attack. But much still needs to be done in relation to a business' third party vendors and ecosystem which is akin to a *friendly dark web*. Friendly, since it knows an enterprise intimately and (often) has unfettered access to proprietary information. The dark web, because knowingly or unknowingly, an organization's third-party ecosystem can become a source of data leaks, exposures, and breaches. In order to be confident of the cybersecurity standards of third-party contractors in any business, one-time self-proclaimed questionnaire-based 'promise' statements are not sufficient. In the words of James Harrington, author of The Innovation Systems Cycle, *Measurement* - of cyber risks - *the first step that leads to control and eventually to improvement* - can be a respite from the vicious cycle of 'breach and repeat.'

Saket Bajoria, Vice President, Product Management & Customer Success, Americas, Safe Security, US