The Achilles Heel of Data Protection

The Achilles Heel of Data Protection

Health Share of Oregon, the state's largest Medicaid coordinated care organization, exposed personally identifiable information (PII) of 654,362 of its members, including names, addresses, phone numbers, dates of birth, Social Security numbers, and Medicaid ID numbers. The breach did not occur at Health Share of Oregon itself, however. The office of one of its suppliers, GridWords IC, a medical transportation company, was burglarized and a laptop with this data was stolen.

When it comes to data protection, a company's third party vendors are too often its Achilles heel. A company can reinforce its own security posture with the latest and greatest technology, but it still has to provide access and share information with its suppliers, and its suppliers' suppliers, and so on up the chain. With each degree of separation, the company has less control over its suppliers' security – especially small suppliers with modest security programs. But when there is a data breach, no matter how far along in the supply chain, the company (Health Share of Oregon, in this case) is still accountable.

"No one's personally identifiable information (PII) is safe. Companies can't count on the integrity of their suppliers' and partners' security capabilities", CSO Online says. Expect more companies to demand security audits of their partners, suppliers, and service providers. Third-party breaches are becoming more common, and it shows that any organization's security is only as good as its extended network."

Third Party Vendor Breaches on the Rise

In one of the biggest data breaches in history, hackers stole 40 million credit cards from Target. The hackers were able to access this data by going through its third party HVAC supplier[1]. Nobody remembers the HVAC company's name, but everyone remembers Target. The breach cost Target over $200 million, plus on-going continued reputational damage to this day.

DASB: Protection that follows your data, with a transparent user experience

Today, high-profile data breaches are an almost daily occurrence, and if you read the details, often the root cause is a third party vendor breach. A recent survey[2] found that nearly 60% of companies in 2018 were the victim of third-party data breaches, a notable increase over the previous year. Greatest hits include:

- Quest Diagnostics
- LabCorp
- DoorDash
- Walmart
- Verizon
- Scottrade Bank
- Italian bank UniCredit
- The Republican National Committee
- Deloitte
- Accenture

The last two examples, Deloitte and Accenture, highlight that while the weak- ink can be your mom-and-pop HVAC supplier, large suppliers are also a risk. Deloitte and Accenture are widely regarded as experts in data protection and are both paid handsomely to advise on security. The egregious breaches that they suffered were the pinnacle of embarrassment in third party security.

No Good Solution?

CIOs agree that supplier security breaches are one of the biggest problems in data protection today, however, to date, this appears to be a problem without a no good solution.

Contractual Terms, Auditing, and Compliance

As a first line of defense, enterprises are demanding stronger contractual terms with suppliers, in terms of the security they require of their vendors, and the legal and financial consequences of a breach. This transition is occurring at a glacial pace. Large enterprises already have thousands of vendors and are not in a position to easily re-negotiate contractual terms with all of them. At best, enhanced contractual terms might provide some financial and legal compensation, although even this is highly dependent on the size of the vendor and the jurisdiction in which they would be held accountable. Ultimately, the responsibility of a breach is still borne by the enterprise itself, particularly including the lasting reputational harm(the public remembers your brand, no one remembers the vendor).

Contracts and good-will aren't enough. Moreover, just because a supplier is agreeable and willing, that doesn't mean their data protection measures are up to par. Enterprises are spending more than ever to audit their partners, suppliers, and service providers, but this is extremely costly, and the great irony is that audits today assume antiquated security measures are in place such as disk encryption and DLP, which are far from a guarantee that a data breach would not occur.

To streamline the certification and auditing of vendors, third party registries have emerged that audit and certify vendors for you. One example is Vendorpedia that certifies third party vendors comply with standards such as GDPR, NIST, and ITAR. The idea is that as an enterprise, you would not have to audit all of your suppliers yourself, but simply require any supplier to show proof of certification and audit from one of these registries. But there are many problems here. A third party registry is only useful if it reaches a critical mass of vendors, which will take a long time and may never happen. And even then, at best vendors are attesting to a certain level of compliance, however as any junior security analyst can tell you, compliant does not mean secure.

Technology Options

In terms of technology, some enterprises ship secured laptops to their third parties and require the third parties to only work on those laptops. Others require that their suppliers work in a virtual space using VDI. These solutions are burdensome, slowing down productivity, and simply don't scale across thousands of suppliers.

Digital rights management (DRM) has had a resurgence of lately because it offers an attractive thesis – protect your sensitive e-mails and files and wherever they go. Even if they fall into the wrong hands, they are still protected. The notion is not wrong. Rather than implementing endless levels of audit, compliance and perimeter security, it is reasonable to assume that data will flow into your partners hands, and eventually into the wrong hands, and that the solution is protection that follows the data wherever it travels. Unfortunately, DRM remains a theoretical idea at best, just as it was 20 years ago. In practice, DRM suffers from significant user experience problems, as users are required to classify their data, and access is limited to certain file types, special applications, plug-in's, authentication mechanisms, access controls, etc. Managing this at scale is unwieldy, and nearly impossible once the data starts flowing into suppliers' hands who have different operating systems, applications, versions, and plug-in's. After 20 years of DRM, there are very few success stories.

If only there was a way to protect your data wherever it goes, but with an invisible user experience that does not slow down productivity?

DASB: Protection That Follows Your Data, with A Transparent User Experience

Data Access Security Broker (DASB) is a limitless data protection solution, delivering transparent and persistent data protection. DASB moves access control policies from the storage system of the data to the data itself – from device-centric to data-centric. Data is automatically protected by default, and this protection follows the data and every action that touches the data, even when it moves into a vendor's hands.

Whether inside your company or at partner, vendor, or customer site, a user can only access the data if they have appropriate privileges per the security policy. An administrator can revoke access to the data and change permissions at any time. Malicious or accidentally shared data cannot be accessed by unapproved parties.

In the case of Health Share of Oregon, its vendor GridWorks IC would not have had access to its members PII unless Health Share of Oregon had authorized this on its policy. As soon as it was known that the laptop with this information was stolen, an administrator would have remotely cut access to all protected data, and the malicious actor would have only had access to encrypted blobs, nothing more. Health Share of Oregon would have also had an audit trail of every access attempt on the data, even the stolen, protected, data that was now in the malicious actor's hands, giving them further insight into the incident.

But unlike DRM technology, DASB is completely invisible to the end user, making it fast to implement and easy to scale. DASB imposes no limits on applications, versions, file types, file sizes, repositories, developer tools, workflows, or anything else in the environment, no matter how complex or enterprise specific. Users don't even realize it is there.

DASB Secures Your Enterprise and Your Supply Chain

Companies who rely on third party vendors and suppliers are exposed to a greater level of data breach risk. Unfortunately, all modern companies today fit this description, and the trend is only increasing. The modern enterprise is highly interconnected with a myriad of suppliers, and no matter how strongly you fortify your own security posture, your Achilles heel will always be those third parties with whom you share information.

DASB eliminates this risk. Whether you're a media enterprise like HBO that collaborates with hundreds of suppliers big and small during the production of a series, whether you're a financial services enterprise the leverages third party services from the Deloitte's and Accenture's of the world, a commerce giant like Target that needs HVAC, or a health provider like Health Share of Oregon, DASB persistently protects data by default so that you remain in control, even when information flows into your vendors hands. Even when it inevitably flows into the wrong hands. DASB covers you and your entire supply chain, all while providing a completely transparent experience.

[1] (https://threatpost.com/hvac-integrators billing-connection-led-to-target-breach/104135/)

[2] (https://www.pymnts.com/news/security-and-risk/2018/third-party-data-breaches-cybersecurity-risk/)

About SecureCircle

SecureCircle's Data Access Security Broker (DASB) eliminates data breaches and mitigates insider threats, with no impact to the end-user experience and no modifications to applications and workflows. Data is always protected at rest, in-transit, and in-use; no matter where it is created, consumed, stored, modified, or shared. Headquartered in Silicon Valley, SecureCircle delivers the world's first data-centric protection for a zero-trust world.

SecureCircle®

SecureCircle.com

4701 Patrick Henry Drive
Building 19, Suite B,
Santa Clara, CA 95054
408-827-9100