Data Breaches and Architecture

Today's news is rife with data breaches. Whether it's government personnel records, heath insurer data, banking information, or a compromise of a social media platform; the data itself - not just defacement or disablement of a website - is under direct threat[1].

How does Enterprise Architecture (EA) help keep data safe but also accessible? First off, EA provides frameworks for data modeling and system documentation. This leads to the understanding and visualizations of data flows for various types of data. Next, EA helps build models for data governance—including elements such as data classifications, use cases, and prioritizations which assist in determining how the data should be protected, who should have access to it and how it can be used or manipulated to best effect. With these tools, leaders can best decide where and how to optimize data resilience to achieve the best results for their business.

These basic building blocks – data modeling, governance, and frameworks - also inform other architecture domains: application, security, technology, and business process. With these elements in place, operational risk and potential exposure are better understood, leading to better employment of controls. Ultimately this considerably reduces risk.

Applying the full suite of EA tools minimizes the impact of potential risks to data. This results in keeping the systems and business processes available and ready to be utilized and accessed by authorized individuals, the data used between the systems secure and confidential, and allows those processes to be trusted and an expectation of total integrity maintained.

Commonalities among contemporary companies experiencing breaches include critical parts of the enterprise architecture not being fully performed or missing altogether. For Anthem BCBS, their breach started through spear-phishing and then the use of look-alike malicious domains. EA modeling includes behavioral analysis of network and system access traffic, something that would detect anomalies and prevent unauthorized access through applied processes[2]. Contrary to Anthem, CareFirst, another large insurer, minimized the risk by separating systems and what data they used (including tokenization), and that led to less sensitive information being lost during their breach a few months later.

Recently, two government bodies experienced very different results from system breaches. One used EA techniques and tools, gaining resiliency to the breach. The other serves as a lesson on the consequences of siloed architecture:

---

[1] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

[2] http://www.forbes.com/sites/frontline/2015/02/24/behavioral-analysis-could-have-prevented-the-anthem-breach/

The Internal Revenue Service (IRS) had a publically facing application that malicious actors used to file false tax refunds. Even though abuse of the system occurred, security architecture measures such as monitoring detected and reduced the consequences because the activity was outside known business operational rules. 7.5% of the data was used to file fax tax returns without being flagged outright, but demonstrates a percentage that is far less than similar breaches directly due to security threat modeling and response being part of the overall system architecture.

Compare the IRS to the Office of Personnel Management (OPM). OPM encountered a larger breach of sensitive information earlier this year, resulting in significant impact. Reporting from OPM asserted[3] that the compromised systems were adequately protected[4]. Unfortunately a data governance model was not in effect – evidenced by data being misclassified[5]. The breach was discovered, not by well-architected process, but through an outside vendor that collected and analyzed indicators of compromise, which remained latent for months[6]. This demonstrates a lack of cohesion of all the various architecture domains of data, application, technology, security and business that could have identified cross-domain control gaps to prevent or mitigate this kind of incident.

As noted above, leveraging enterprise architecture increases resiliency and decreases negative impacts. Appropriate integration of EA when developing a system or solution directly reduces the potential risk to your organization. The sharing of best practices, development of appropriate policies, and the establishment of frameworks/governance models helps keep our organization and the words "data breach" out of the news. EA ensures synergies among different architecture domains ensuring resiliency to risk while maximizing efficiency.

---

[3] http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/
[4] http://arstechnica.com/security/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/
[5] http://arstechnica.com/security/2015/07/call-it-a-data-rupture-hack-hitting-opm-affects-21-5-million/
[6] http://www.opm.gov/news/latest-news/announcements/frequently-asked-questions/