ABERDEEN GROUP

Security for Your Cloud-Based Web Applications: For Success, Focus on What You Do Best

April 2017

Aberdeen Group's research shows how enterprises are choosing to focus their finite resources on what they do best, and to partner for the rest. Enterprise application development teams focus on their own applications and data, leveraging **public cloud service providers** for computing infrastructure and **security service providers** for mitigating cyber security risks.

Web Applications are a Common Target for Attack, and the Leading Source of Confirmed Data Breaches

Let's start with the bad news up front: the best available empirical data shows not only that cyber security attackers like to target your **web applications**, but also that web applications have been their number one path to success.

As described in the Verizon *Data Breach Investigation Report* (DBIR) series, based on the empirical investigations of more than 64,000 incidents — and nearly 2,300 confirmed data breaches — it's clear that web applications continue to be a favorite target for attackers:

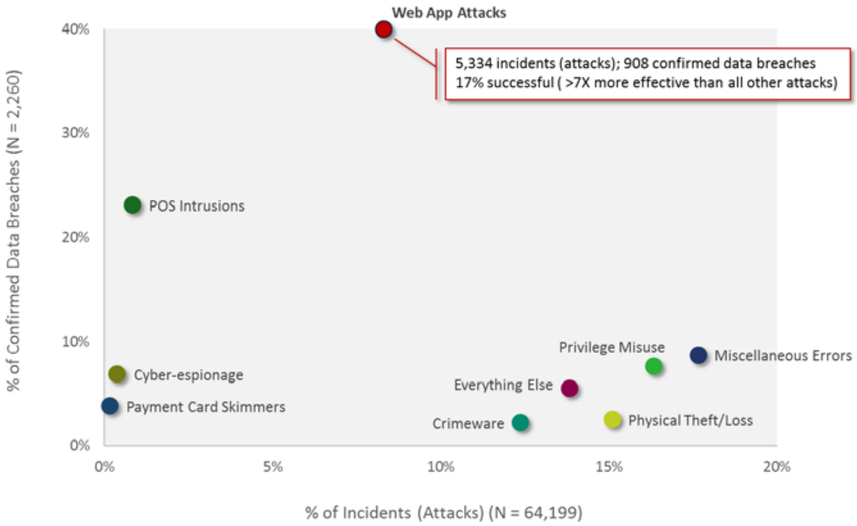
- 5,334 incidents (8.3% of total attempts investigated)
- 908 confirmed data breaches (39.9% of total successes)
- 17% success rate

Historically, attacks against web applications have been **more than seven times more effective** for the bad guys than those on all other leading categories of targets (see Figure 1).

➔ Read the full report: *Security for Your Cloud-Based Web Applications: Why, and How*

Historically, attacks against web applications have a 1 in 6 likelihood of succeeding — which is **more than 7x more effective for the bad guys** than attacks on all other leading targets.

Figure 1: Attacks Against Web Apps are the Most Successful



Source: Adapted from Verizon 2016 DBIR; Aberdeen Group, April 2017

Why Security for Your Web Applications Matters: Understanding and Quantifying Your Risks

But the *likelihood* of a successful attack on your web applications is only one part of the puzzle. To make an informed **business decision** about security, organizations need to understand and appreciate the **risk** to their web applications — and risk is always defined not only in terms of the likelihood of occurrence, but also in terms of the *business impact* if an incident does in fact occur.

Based on empirical data for likelihood and business impact, Aberdeen has used analytical techniques (e.g., Monte Carlo modeling) to *quantify* estimates for selected risks to web applications, including the risk of **data breaches**, the risk of **DDoS attacks**, and the risk of **malicious bots**:

- **Data breaches:** Based on a compromise of *1M to 10M records*, the business impact of a single data breach in the *private sector* (across all industries) is estimated to be **between $135,000 and $795,000**, with a **median of about $425,000**. For specific industry sectors such as *retail*, *accommodation*, and *healthcare*, the risk is much higher.

The risks to your web applications are material, as Aberdeen's analysis helps to quantify — and this demands deliberate *business decisions* regarding whether to accept them, or to take steps to manage them to an acceptable level.

- **DDoS attacks:** Enterprises have *greater than 50% likelihood* of experiencing DDoS attacks, with a median total attack duration of **about 200 hours per year**. Under the status quo protections (i.e., *network firewall*, *intrusion detection*), the median annualized business impact of disruptions from DDoS attacks is **about 2.2% of annual revenue**.
- **Malicious bots:** The annualized business impact of malicious bots is estimated to be **between 1.5% and 6.4% of annual revenue**, with a **median of about 3.7%**.

Why Your Web Apps are Vulnerable: Complexity and Change

It's worth noting some of the high-level reasons that your web applications are more vulnerable, which in turn enables attackers to sustain such significant levels of success. In Aberdeen's view, a perfect storm of **complexity** and **change** is a dominant factor, in multiple dimensions:

- In the foundational **computing infrastructure**
- In modern **application development practices**
- In sustaining the requirements for **security**, **privacy**, and **regulatory compliance**

Complexity and Change in the Computing Infrastructure

Aberdeen Group's visibility into current technology installations for a simple six-layer "stack" of computing infrastructure included *336 products* from *57 vendors*, for *more than 1.6 billion unique permutations*. Integrating, optimizing, and maintaining the exponentially growing complexity of your foundational computing infrastructure is obviously *important*. For most organizations, however, your **applications** and **data** are what's truly *strategic* — and therefore the primary focus of attention and innovation.

For this reason, organizations are increasingly choosing to rely on leading **public cloud service providers** (e.g., Amazon Web

Services) to do what service providers know best (i.e., *integration* and *optimization* of the lower levels of the computing infrastructure stack, at *large scale*), and to focus their own resources on what enterprises know best (i.e., their own applications and data).

Complexity and Change in Application Development Processes

A second major factor in the vulnerability of web applications is the complexity of **changing application development practices**. Organizations are increasingly moving:

- ➔ Away from a *traditional, sequential approach* to application development, with a focus on making a large collection of changes on a fixed release schedule (i.e., analysis, design, implementation, testing, release, deployment, and ongoing support and updates)
- ➔ Toward a *flexible, continuous, highly responsive approach* to application development, with a focus on responding to customer needs and market opportunities by making many small changes quickly (e.g., Agile, Scrum, DevOps)

These changes are accelerating the development of new web applications using the infrastructure of public cloud service providers. They are also increasing the perceived "relevance gap" for traditional approaches to IT and information security. The high frequency of code changes means that many organizations are accepting (or worse, ignoring) an inappropriate level of risk, and leaving themselves with limited means of visibility and control.

Acceleration of the development of new web applications using the infrastructure of public cloud service providers is also increasing the perceived "relevance gap" for traditional approaches to IT and information security.

In addition, organizations are leveraging **multiple sources** of application development and functionality, by integrating their own development with third party vendors, systems, and libraries. Third party vulnerabilities are more likely to also become your vulnerabilities, with the potential to be exploited by the attackers.

Complexity and Change in Security, Privacy, and Compliance

Finally, the challenge of sustaining the requirements for security, privacy, and regulatory compliance has become considerably more complex over time, and contributes to the ongoing vulnerability of web applications. This is true for organizations of all sizes, with ever-increasing attention demanded for:

- Keeping up with the technical landscapes for the latest **threats** and **vulnerabilities**
- Ensuring that networks, systems, and applications are **protected**
- **Certifying** that networks, systems, and applications are compliant with policies, and with regulatory requirements
- **Integrating** and **managing** multiple tools and point solutions into a comprehensive security "stack"
- **Monitoring**, **detecting**, **investigating**, and **responding** to security incidents in a timely way, around the clock

Just as it is with the foundational computing infrastructure, it's not necessarily that organizations aren't *capable* of achieving a high level of maturity in the governance and management of security controls for their web applications — it's that they generally choose to prioritize their finite resources on other, more strategic activities. For example, it's common for the "rewarded risks" of functionality and time-to-market requirements for key business applications to trump the "unrewarded risks" of security, privacy, and compliance.

For this reason, organizations are increasingly choosing to rely on the specialized expertise, integration, scale, visibility, and continuous monitoring of **security service providers**, across the full stack of security relevant for web applications: *network*, *platform*, *application*, and *analytics*.

Organizations that move their application workloads to public cloud service providers are outsourcing the *architecture* and *implementation* of their foundational computing infrastructure, but to be very clear, they are not fully outsourcing the governance and operations of *security*, *privacy*, and *compliance*.

Enterprises still need to understand and address their **ongoing, shared responsibilities** for the security of their cloud-based web applications.

Ignoring your risks is the same as accepting them, only worse — in the sense that you are not making a deliberate business decision.

Rewarded risks have to do with *enabling assets***,** *maximizing upside***,** and *creating value*.

Unrewarded risks have to do with *defending assets***,** *minimizing downside,* and *protecting value*.

Organizations are finding successful ways to deal with unprecedented rates of complexity and change, by using the time-tested approach of ***focusing on what you do best*.**

How Organizations are Choosing to Deal with Increasing Complexity and Change: For Success, Focus on What You Do Best

This is the key point: organizations are finding successful ways to deal with unprecedented rates of complexity and change, by using the time-tested approach of **focusing on what you do best**:

- **Enterprise application development** teams are focusing their own resources on the most strategic aspects of the computing infrastructure stack: their own applications and data.
- **Leading public cloud service providers** deliver the architecture, integration, optimization, and operational aspects of the essential lower levels of the computing infrastructure stack, at large scale.
- **Security service providers** deliver the specialized expertise, integration, scale, visibility, and continuous monitoring across the full stack of security for web applications: *network*, *platform*, *application*, and *analytics*.

Aberdeen's benchmark research provides useful insights into this last point, and highlights the growth in the use of security service providers. Current deployments of security solutions are skewed towards traditional, in-house implementations — but given the discussion above, it's not surprising that planned growth overwhelmingly favors the use of outsourced security solutions.

For example, consider an analysis of current deployments and planned deployments for 180 organizations participating in Aberdeen's benchmark research study, for the following "stack" of security solution categories that are relevant to cloud-based web applications:

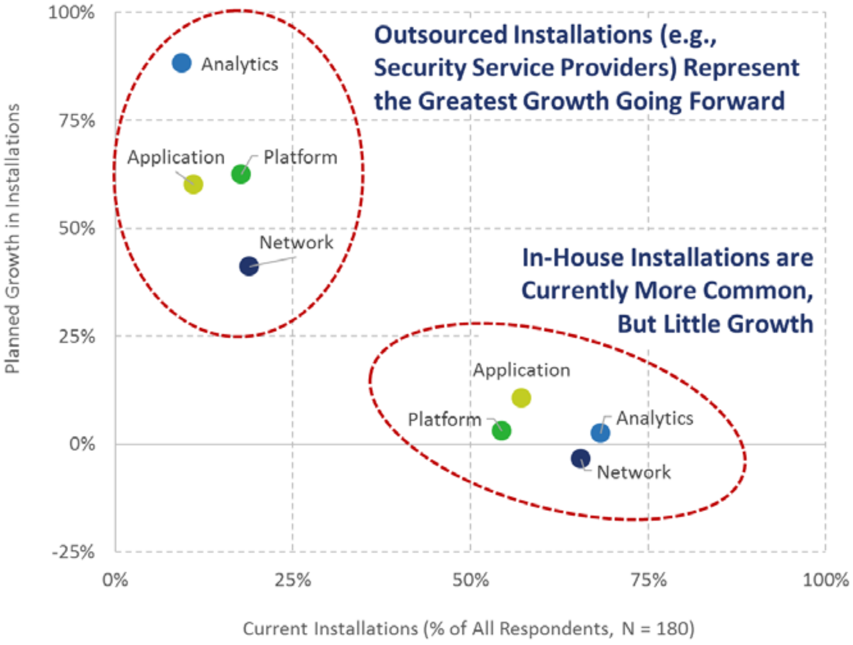
- **Network** — e.g., *firewalls*, *intrusion detection*
- **Platform** — e.g., *network monitoring*
- **Application** — e.g., *web application firewalls*

- ➔ **Analytics** — e.g., *log management, security information and event management* (SIEM)

As seen in Aberdeen's dataset, roughly 50% to 75% of current deployments of this stack of security solutions are traditional, in-house implementations. This compares with roughly 10% to 25% of current deployments with external security service providers. But with respect to planned deployments, virtually all the growth among Aberdeen's respondents favors the use of external partners (Figure 2).

Virtually all the growth among Aberdeen's respondents favors the use of security service providers.

Figure 2: For a "Stack" of Security Solutions Relevant to Cloud-Based Web Applications, Security Service Providers Represent the Greatest Growth



Source: Aberdeen Group, April 2017

Enterprise application development teams focus their resources on their own applications and data.

Leading public cloud service providers deliver the architecture, integration, optimization, and operational aspects of the essential lower levels of the computing infrastructure stack, at large scale.

Security service providers deliver the specialized expertise, integration, scale, visibility, and continuous monitoring across the full stack of security for cloud-based web applications: *network*, *platform*, *application*, and *analytics*.

Summary and Key Takeaways

- ➔ Your web applications are a **common target for attack**, and **the leading source of confirmed data breaches**.
- ➔ The **risks to your web applications** — e.g., the risk of *data breaches*; the risk of *DDoS attacks*; the risk of *malicious bots* — are **material**. This demands deliberate **business decisions** regarding whether to accept them, or to take steps to manage them to an acceptable level.
- ➔ Increasing **complexity** and **change** — e.g., in the foundational *computing infrastructure*; in modern *application development practices*; in requirements for *security*, *privacy*, and *regulatory compliance* — contribute to the vulnerability of your web applications.
- ➔ In response, market trends show that **organizations are focusing on what they do best**, and leveraging the third-party expertise of leading **public cloud service providers** and **security service providers** for other important activities.

Author: Derek E. Brink, CISSP
Vice President and Research Fellow, Information Security and IT GRC

About Aberdeen Group

Since 1988, Aberdeen Group has published research that helps businesses worldwide to improve their performance. Our analysts derive fact-based, vendor-neutral insights from a proprietary analytical framework, which identifies Best-in-Class organizations from primary research conducted with industry practitioners. The resulting research content is used by hundreds of thousands of business professionals to drive smarter decision-making and improve business strategies. Aberdeen Group is headquartered in Waltham, Massachusetts, USA.