ABERDEEN GROUP

THE STATE OF SMB SECURITY RISKS: WHY MOST SMBS ARE LOOKING TO MSSPS

November 2016

For small and mid-size businesses (SMBs) of up to 1,000 employees, Aberdeen Group's analysis shows that the risk of a single data breach is significantly higher than it is for larger organizations — by about 63%. Not surprisingly, virtually all planned growth among SMBs is based on moving away from in-house implementations, in favor of using managed security service providers (MSSPs).

Definitions

A **security incident** refers to any event that attempts to compromise the *confidentiality*, *integrity,* or *availability* of an information asset.

A **data breach**, or **data compromise**, refers to a security incident which results in the confirmed disclosure of an information asset to an unauthorized party.

The **risk** of a data breach must always be described in terms of both the *likelihood* that it may occur, as well as the *business impact* if it actually does occur.

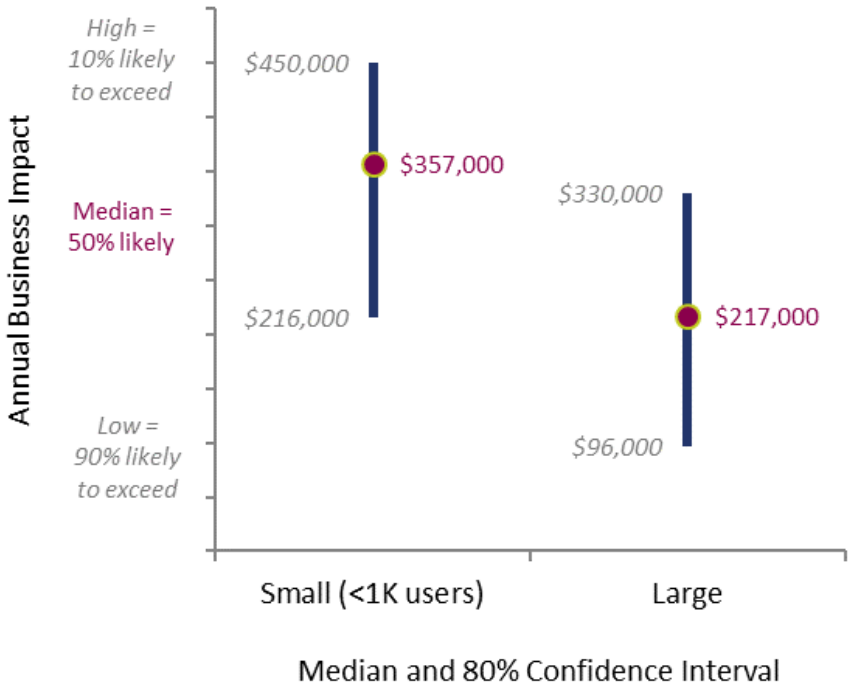
Small and Mid-Size Businesses (SMBs) Need to Do Something About Their Security-Related Risks

In its 2016 research report *Small Business, Bigger Risk: Quantifying the Risk of a Data Breach,* Aberdeen Group makes use of empirical data from the well-known Verizon Data Breach Investigations Report (DBIR) series — including the *likelihood* of a data breach, and estimates for the *cost* of a data breach — to quantify the **risk** of a data breach, as a function of *industry*, the *number of records compromised*, and the *size of the organization*.

Based on Aberdeen's updated analysis, using findings from the Verizon 2016 DBIR, the risk of a single data breach of between 100,000 to 1,000,000 records is significantly higher — by about 63% — for SMBs of up to 1,000 employees than it is for larger organizations (see Figure 1):

- ➔ For SMBs, there's a **90% likelihood** of a single data breach costing **more than $216,000**, and a **10% likelihood** of a single data breach costing **more than $450,000**, with a **median** (50% likelihood) cost of **about $357,000**.
- ➔ For larger organizations, the cost of a single data breach is **between $96,000 and $330,000** (this is the *80% confidence interval*), with **a median** cost of **about $217,000**.

Figure 1: Smaller Enterprise, Bigger Risk — Cost of a Single Data Breach, Based on a Compromise of 100K to 1M Records

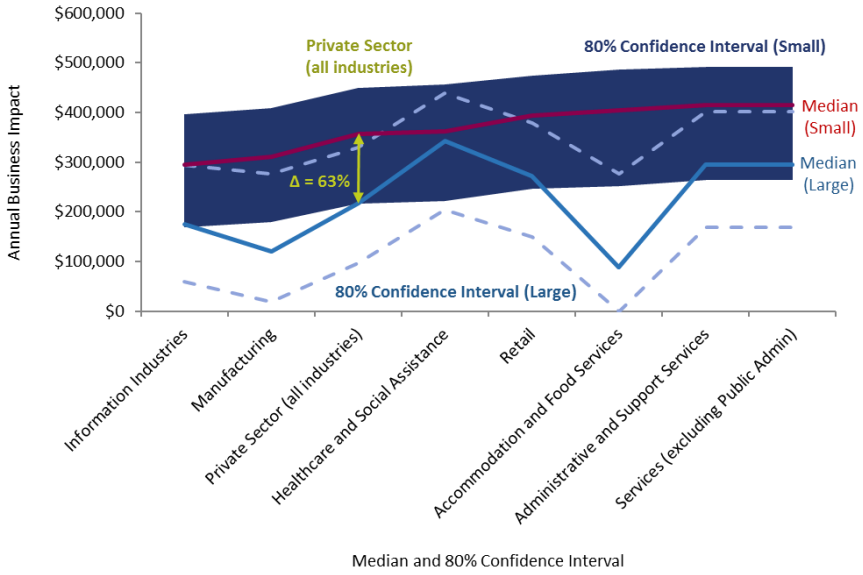


Source: Monte Carlo analysis, based on empirical data from Verizon DBIR; Aberdeen Group, November 2016

Figure 2 depicts the risk of a single data breach for the **private sector** (across all industries), as well as for seven selected sectors for which SMBs have higher risk. Again, this is based on a compromise of 100,000 to 1,000,000 records:

- ➔ Information Industries: 69% higher
- ➔ Manufacturing: 159% higher
- ➔ Healthcare and Social Assistance: 6% higher
- ➔ Retail: 45% higher
- ➔ Accommodation and Food Services: 354% higher
- ➔ Administrative and Support Services: 41% higher
- ➔ Other Services (excluding Public Admin): 41% higher

Figure 2: Smaller Enterprise, Bigger Risk — Cost of a Single Data Breach for Selected Industry Sectors, Based on a Compromise of 100K to 1M Records



Source: Monte Carlo analysis, based on empirical data from Verizon DBIR; Aberdeen Group, November 2016

Why SMBs Have a Higher Risk of Being Compromised

A significant factor for the higher risk SMBs have over larger organizations is that information technology and information security technologies have become increasingly **complex**. This is true for organizations of all sizes, of course, with ever-increasing attention demanded for:

- ➔ Keeping IT infrastructure properly configured, patched, and up-to-date
- ➔ Achieving and sustaining compliance requirements for security and privacy
- ➔ Keeping up with the latest security threats and vulnerabilities landscapes
- ➔ Ensuring that IT infrastructure and sensitive data are well-protected

➔ Monitoring, detecting, investigating, and responding to security incidents in a timely manner

Small and mid-size businesses often lack the **resources** (both bandwidth of existing personnel, and specialized technical expertise) and the tactical **focus** to perform well at these activities, because their primary, strategic focus is naturally on running and growing their business — not on security, compliance, privacy, and risk. It's not that SMBs aren't *capable* of achieving a high level of maturity in the governance and management of technical, administrative, and physical security controls; it's that they generally choose to prioritize other activities.

It's not that SMBs aren't *capable* of achieving a high level of maturity in the governance and management of technical, administrative, and physical security controls; it's that they generally choose to prioritize other activities.

These factors combine to contribute to SMBs being an attractive target for attackers, with a correspondingly higher likelihood of success. In addition, small business leaders often make false assumptions about risk, e.g., "data breaches won't happen to us," and "we don't have anything of value that attackers would want." In truth, however, small businesses may represent extremely high-value targets for attackers, as they represent a much easier beachhead and conduit for attackers to gain access to larger organizations in the supply chain.

SMBs Don't Have to Do IT Alone: A Classic "Build vs. Buy" Decision

In a 2014 research report on Managed Security Services, Aberdeen asked a rhetorical question that's just as relevant today: Even if a given SMB is capable of traditional, do-it-yourself integration of on-premises information security solutions using in-house resources, is it really better off doing IT on its own — or would it be better off leveraging the expertise, scale, and scope of a specialized third-party service provider?

An analysis of the respondents in Aberdeen's benchmark research studies provide compelling evidence of the SMB's answer. Not surprisingly, current deployments of information security solutions are skewed strongly towards in-house solutions. But

virtually all planned growth favors the use of **managed security service providers** (MSSPs).

MSSPs offer services such as management, monitoring, testing and incident response for one or more specific information security solution categories (e.g., *intrusion detection / prevention*, *log management*, *security incident and event management*, *network monitoring*, *endpoint protection*, and so on). MSSP functionality may be delivered over the Internet, by on-premises systems (e.g., appliances which are remotely managed), or through a hybrid model. And "build vs. buy" is by no means an all or nothing proposition — i.e., SMBs may choose to implement some security capabilities in-house, side-by-side with other capabilities from trusted MSSPs.

Three Illustrative Examples of SMBs Choosing MSSPs: Internal, Perimeter, and External

To illustrate the strong movement of SMBs towards choosing MSSPs, Figure 3 summarizes the current deployments and planned deployments for 54 small and mid-size businesses participating in Aberdeen's benchmark research study, for three representative information security categories:

- ➔ *Internal*: endpoint protection
- ➔ *Perimeter*: intrusion detection / prevention
- ➔ *External*: log management / security information and event management

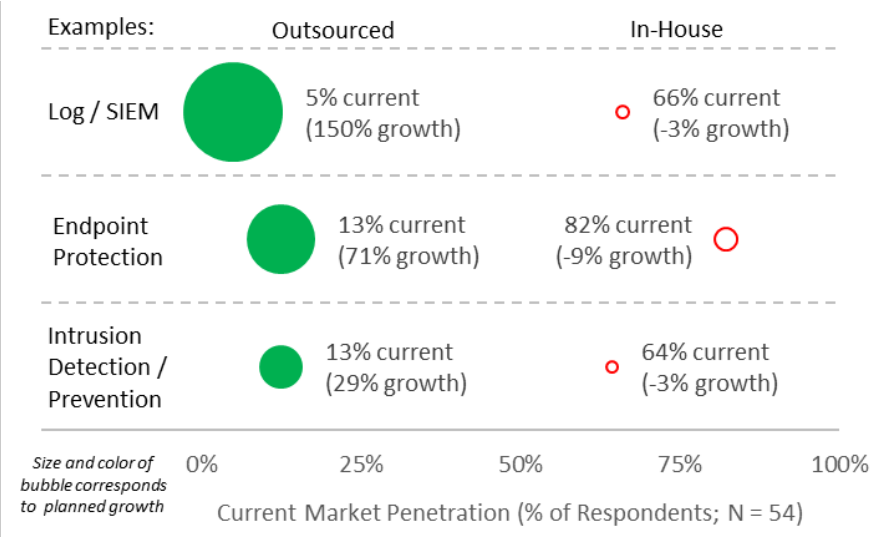
As seen in Aberdeen's dataset, roughly 60% to 80% of current deployments are in-house implementations, compared to roughly 5% to 15% of current deployments with third-party service providers. But with respect to planned deployments of information security solutions, literally all the growth among SMBs favors the use of MSSPs.

Log management solutions address the process of generating, transmitting, aggregating, storing, and eventually disposing of log data.

Security information and event management (SIEM) solutions are generally complementary to log management, in that they are used to *ingest*, *interpret*, and *take action* on security-related log, information, event, flow, session, threat intelligence, and other data from a diverse range of sources.

With respect to planned deployments of information security solutions, literally all of the growth among SMBs favors the use of MSSPs.

Figure 3: For Small and Mid-Size Business, All Planned Growth Favors Managed Security Service Providers



Source: Aberdeen Group, November 2016

Summary and Key Takeaways

- Empirical data shows that **small and mid-size businesses actually have higher security-related risks** than larger organizations.
- Ignoring their security-related risks is not a viable option for staying in business — **SMBs need to make a deliberate business decision** to accept, transfer, or manage these risks to an acceptable level.
- In the *build* (in-house) vs. *buy* (outsourced) business decision regarding security-related risks faced by SMBs, logic points to an increased use of managed security service providers — and Aberdeen's research findings confirm that SMBs are increasingly following this logic. With respect to planned deployments of information security solutions, literally **all of the growth among SMBs favors the use of MSSPs**.

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.