Quantifying the Value of Firewall Management

October 2016

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

Report Highlights

The surprising complexity of enterprise network firewall infrastructure means that manual management of policies, rules, and configurations is time-consuming and error-prone, which adds operational cost and increases security-related risks. Aberdeen Group's simple Monte Carlo analysis shows that compared to the status quo, the implementation of a firewall management solution corresponds to a median reduction in risk of about 3.6 times, and a median annual return on investment of more than 200 times.

ABERDEEN GROUP

2

Security teams and business leaders should not be complacent about their network firewall infrastructure — which for many has grown surprisingly complex, adding significant operational cost and increasing security-related risks. Investments in visibility, intelligence, integration, and automation can help enterprises to win back control over their firewall sprawl.

➔ Related Research: *Firewall Sprawl: How Complexity is Adding Cost and Increasing Risk*

The Complexity of Managing Firewalls Adds Cost, Increases Risk

In its research report on *Firewall Sprawl: How Complexity is Adding Cost and Increasing Risk* (October 2015), Aberdeen Group examined more than 13,000 current network firewall installations — an analysis which revealed a surprising degree of **complexity**. Nearly half (46%) of all enterprises in this market snapshot are faced with multiple sites and / or multiple firewall vendors, each of which in turn has numerous firewall *policies*, *rules*, and *configurations* that must be established, implemented, and maintained over time. If managed manually (or with multiple, inconsistent tools), the complexity of the status quo **adds significant operational cost** and **increases security-related risks**.

In Aberdeen's view, the cornerstone to winning back enterprise control over this firewall sprawl is having continuous, real-time **visibility** into the actual policies, rules, and configurations that are currently in place throughout your network firewall infrastructure:

- ➔ Firewall policies and rules may be conflicting, out of date, redundant, or the result of ad hoc decisions that bypassed the normal approval process.
- ➔ Firewall configurations may be incorrect or out of date, either as a result of unapplied patches and updates, or from simple human error.

Making informed decisions about these issues requires having the necessary *context*, which should be based on *directly relevant* **intelligence** about your network. In addition, **integration** with a wide range of network firewall products, and **automation** of the workflows for configuration changes and policy updates — which is designed to provide a high level of assurance that these important tasks are accurately and consistently carried out — are both also essential to realizing the *operational benefits* of **lower cost** and the *strategic benefits* of **reduced risk**.

3

Definitions

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

Unplanned **downtime** (or **slowdown**) refers to a security incident which results in the computing resources that the attacker is targeting being unavailable to their intended users (e.g., as a result of a **denial-of-service** attack).

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 security-related incidents such as network downtime, network slowdown, or data breaches is properly described in terms of the *likelihood* that they may occur, as well as the *business impact* if they actually do occur.

Quantifying the Operational Cost and Security-Related Risks of Managing Network Firewalls, Under the Status Quo

As described in the *Firewall Sprawl* report, dealing with the increased complexity of multiple sites, vendors, devices, policies, rules, and configurations has a ripple effect on both the operational cost and the security-related risks of managing an organization's network firewall infrastructure:

- Increased complexity corresponds to a non-linear increase in the **operational cost** of managing firewall policies, rules, and configurations throughout the enterprise, based on the longer time it takes to *review*, *check*, *approve*, *implement*, *test*, and *validate* these adds or changes. Simply put, complexity requires more time and more staff.
- In turn, greater complexity contributes to an increased likelihood of **inconsistencies**, **errors**, and **omissions** in these tasks — which increases the number of **threats** and **vulnerabilities** that are relevant to the organization's network infrastructure and network-dependent resources. Simply put, complexity increases the *likelihood* that these vulnerabilities may be successfully exploited, with the corresponding *business impact*.
- The **business impact** of security-related incidents includes the *cost of responders* (e.g., IT staff, Incident Response, Forensics, Help Desk staff); the fraction of *network-supported revenue lost* during the period of downtime or slowdown; the fraction of *user productivity lost* during the period of downtime or slowdown; and the incremental *cost of data breaches*.

To quantify the operational cost and the security-related risks of managing network firewall infrastructure under the status quo — and to quantify the value of an incremental investment in a firewall management solution for reducing cost and risk —

4

Monte Carlo Models and Risk

In a **Monte Carlo** analysis, each variable in a calculation is expressed not as a single, static value — but as a *range* (lower bound, upper bound) and a *shape* (probability distribution). The relevant calculations are then carried out based on a randomly selected value from the probability distribution for each variable, over many (say, 10,000) independent iterations.

In doing so, the results of the analysis are also expressed as a range and distribution (as opposed to as a single, static value). The results can then be represented in terms of both *how likely* and *how much* — i.e., in terms of **risk**, as risk is properly defined.

This provides security professionals with exactly what they need to quantify estimates that are useful for **informing a better business decision about risk**, in spite of the inherent **uncertainties** in these matters. It also provides a useful tool for addressing fundamental business questions such as:

- The **cost** and **risk** of managing network firewalls, under the status quo
- **The value of an incremental investment** in firewall management, for reducing cost and risk

Aberdeen has developed a simple **Monte Carlo** model, using the standard functionality of Microsoft Excel. Personalization of **contextual** factors is enabled by supporting the selection of:

- ➔ The *number of sites* with firewall installations (across the entire enterprise)
- ➔ The *number of firewall vendors* (across all sites)
- ➔ The total *number of devices*
- ➔ The amount of *annual revenue* supported by the network
- ➔ The *number of users* supported by the network
- ➔ The *industry* sector
- ➔ The *number of data records* at risk from unauthorized network access

In addition, the model makes use of Aberdeen's estimates for the lower bound, upper bound, and distributions for three high-level **factors**: the *operational cost* of managing firewalls; the *risk* of network downtime or slowdown; and the *risk* of data breaches.

- ➔ The **operational cost** of managing firewalls is based on estimates for the *number of changes* to policies, rules, and configurations throughout the enterprise; the *time it takes* to review, check, approve, implement, test, and validate these adds or changes; and the *fully-loaded cost* of operational staff.
- ➔ The **risk of downtime or slowdown** is based on estimates for the *time the network is negatively affected* by security-related issues (e.g., downtime or slowdown); the *number and cost* of full-time equivalent responders (e.g., IT staff, Incident Response, Forensics, Help Desk staff); the amount of *annual revenue* supported by the network, and the *fraction of network-supported revenue lost* during the

5

"ALE-Style" Calculations and Risk

Annualized Loss Expectancy (ALE) is a pretty common approach to quantifying security-related risks (for example, you're likely to find it on the CISSP exam).

The formula is **ALE = SLE * ARO**, where:

- **ALE** = Annualized Loss Expectancy
- **SLE** = Single Loss Expectancy = Asset Value * Exposure Factor
- **ARO** = Annual Rate of Occurrence

The good news is that ALE-style calculations incorporate both *likelihood* and *business impact*, i.e., ALE talks about risk in the correct way. The problem is that this approach is based on a level of certainty that just doesn't exist — and results in a falsely precise "answer" that simply isn't credible. If we could compute the various factors of risk with this kind of precision, it wouldn't be a risk at all: it would be a fact!

A Monte Carlo analysis uses the same basic approach, while also addressing the inherent uncertainties.

period of downtime or slowdown; the *number of users* supported by the network, and the *fraction of user productivity lost* during the period of downtime or slowdown; and the *fully-loaded cost* per user.

➔ The **risk of a data breach** is based on estimates for the *number of data records* at risk from unauthorized network access; the *likelihood* of experiencing at least one data breach (as a function of *industry*, based on empirical data from the Verizon Data Breach Investigation Report); if successfully breached, the *number of data breaches* experienced per year; and the *percentage of data breaches* resulting from attacks on the network (also based on empirical findings from the Verizon DBIR).

Traditional **"ALE-style"** calculations — which would make use of known, fixed, certain quantifies for each of these variables — would also present the results as a known, fixed, certain quantity. The absurdity of this approach is the kind of "crackpot rigor" that has led so many security professionals and business leaders to abandon attempts to quantify security-related costs and risks, in favor of purely qualitative models (e.g., red / yellow / green "heat maps"). Unfortunately, these really don't move the dial for risk-based decisions that are primarily made on intuition and gut feel.

Aberdeen's Monte Carlo model addresses these issues, as illustrated by the following estimates for the operational cost and security-related risks of managing firewalls for a mid-size network infrastructure (three firewalls, three sites, two different vendors) in the private sector, which supports $100M in annual revenue and 1,000 users:

➔ The *median* annualized business impact of managing firewalls in this scenario is **about $4,470,000**.

➔ There's a *90% likelihood* that the total annualized business impact is **more than $1,350,000**, and a *10% likelihood* that

Under the status quo, the total annualized business impact of managing firewalls for a mid-size network infrastructure (three firewalls, three sites, two different vendors), in the private sector, which supports $100M in annual revenue and 1,000 users, is estimated to be **between $1,350,000 and $8,910,000**, with a most likely value of **about $4,470,000**.

Said another way, the total annualized business impact in this scenario is estimated to be **between 1.4% and 8.9% of annual revenue**, with a most likely value of **about 4.5%**.

the total annualized business impact will be **more than $8,910,000** (this range is the *80% confidence interval*).

➔ Expressed another way, the total annualized business impact in this scenario is estimated to be **between 1.4% and 8.9% of annual revenue**, with a most likely value of **about 4.5%**.

Based on these estimates from their subject-matter experts and trusted advisors, some business decision-makers may choose to accept the risk. Others may find this level risk to be unacceptably high, and ask for recommendations on managing it to an acceptable level. As always, the primary role of the information security professional is to *identify*, *assess*, and *communicate* the risk in a way that helps the owners of the risk reach a *better-informed business decision*.

Quantifying the Value of an Investment in Firewall Management

A straightforward extension to Aberdeen's Monte Carlo model can provide invaluable insights into the very natural follow-on question of the business decision-maker: how would an investment in a **firewall policy management** solution quantifiably reduce operational costs and security-related risks? This requires ranges and distributions for just two additional variables:

➔ The **relative effectiveness** of firewall management using a solution provider, as compared to the status quo – i.e., a much *faster* and *more accurate* ability to review, check, approve, implement, test, and validate adds or changes to firewall policies, rules, and configurations.

➔ The **incremental annualized cost** of a firewall management solution, which must be tallied as part of the business impact in the "after" scenario — i.e., we need to count both the costs as well as the benefits.

No Model is Perfect — But Some Models Are Useful

It can be tempting — especially for technically-oriented information security professionals — to get carried away with building models that attempt to be more even more precise, or which incorporate even more factors of likelihood and business impact.

For example, what about the opportunity cost of users, above and beyond their lost productivity from network downtime or slowdown? Or the opportunity cost of network administrators, from freeing up their time to work on other tasks after implementing firewall management? Or how about the negative impact on reputation and brand that may result from data breaches, or poor network availability and performance?

Keep in mind that the objective is to **help make better business decisions about risk**, in the face of inherent *uncertainties*. If it turns out that additional granularity is really needed to make a decision, it can always be added — but if a decision can be made based on a more *conservative*, *understated* estimate of cost and risks, why make it more complex than necessary? Einstein was right: we should keep things as simple as possible, but no simpler.

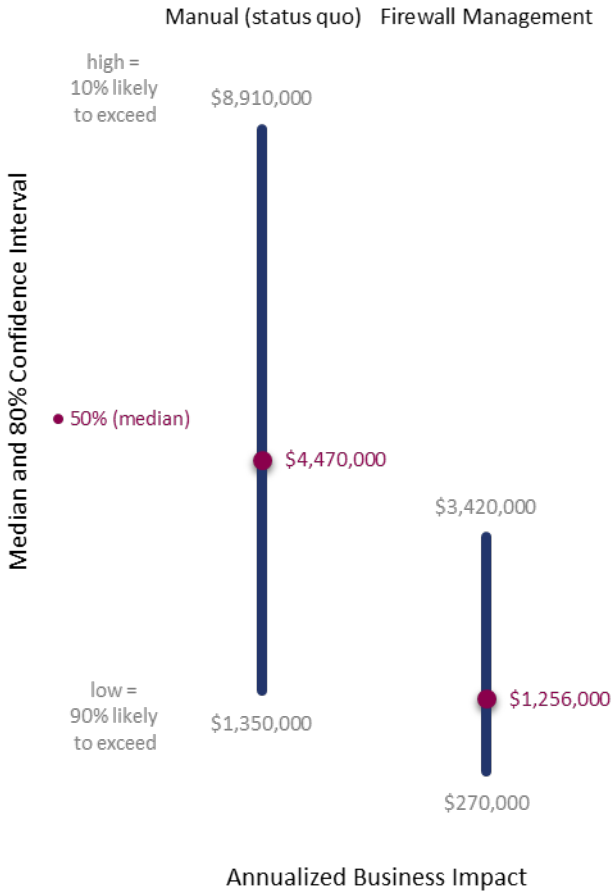
Based on estimates for these two variables shared with Aberdeen courtesy of firewall management solution provider FireMon, Aberdeen's Monte Carlo model quantifies the value of firewall management in the same illustrative scenario:

- After the implementation of firewall management, the total annualized business impact of managing firewalls is estimated to be **between $270,000 and $3,420,000**, with a median of **about $1,256,000**.
- Expressed another way, the total annualized business impact in this scenario is estimated to be **between 0.3% and 3.4% of annual revenue**, with a most likely value of **about 1.3%**.
- This represents a median reduction in risk of **about 3.6 times**, net of the incremental investment in the firewall management solution, and a median annual return on investment of **more than 200 times**.

A visualization of the total annualized business impact of managing firewalls in this scenario, comparing the "before" and "after" cases, is provided as Figure 1.

Aberdeen's Monte Carlo analysis shows that compared to the status quo, the implementation of a firewall management solution corresponds to a median **reduction in risk of about 3.6 times**, and a median annual **return on investment of more than 200 times**.

Figure 1: Quantifying the Operational Cost and Security-Related Risks of Managing Network Firewalls, and the Value of Firewall Policy Management



Source: Based on $100M revenue and 1K users; Aberdeen Group, October 2016

Additional Insights: Breaking Down the Business Impact

One additional benefit of modeling the three high-level factors of the *operational cost* of managing firewalls, the *risk* of network downtime or slowdown, and the *risk* of data breaches is that it provides additional insights into which makes the greatest contribution to the total annualized business impact. As seen in Table 1 and again in Figure 2, it turns out that the **lost productivity of users** as a result of network *downtime* or *slowdown* is by far the

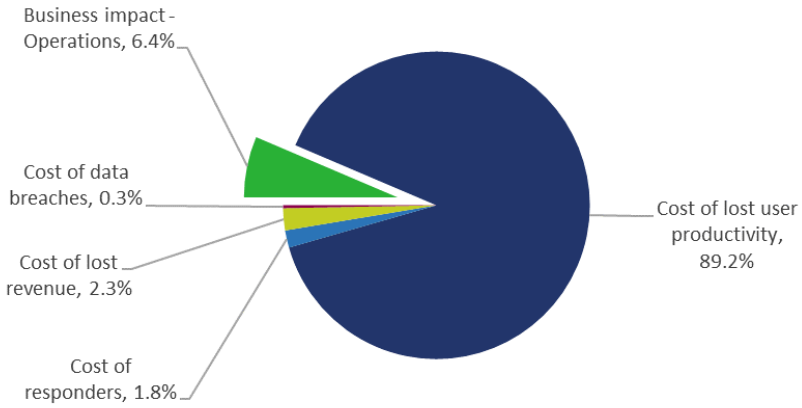
biggest factor, followed by the **operational cost** of managing adds and changes to firewall policies, rules, and configurations across a complex network infrastructure. Think of these figures as a drill-down on the red circles that represent the median (50% likelihood) level of risk as shown in Figure 1.

Table 1: Drill-Down on the Median (50% Likely) Level of Risk

Median Business Impact ($ / year)	Manual (status quo)	Firewall Management
Business impact - Operations	**$276,000**	**$76,000**
Cost of lost user productivity	$3,865,000	$1,039,000
Cost of responders	$79,000	$21,000
Cost of lost revenue	$100,000	$27,000
Cost of data breaches	$13,000	$4,000
Business Impact - Security	**$4,057,000**	**$1,091,000**
Investment in Firewall Management		$15,000

Source: Based on $100M revenue and 1K users; Aberdeen Group, October 2016

Figure 2: Total Annualized Business Impact of Managing Network Firewalls is Dominated by the Cost of Lost User Productivity, Followed by the Operational Cost of Managing Policies



Source: Based on $100M revenue and 1K users; Aberdeen Group, October 2016

From the perspective of making a business case for an investment in firewall management, this may be happy news: the primary

argument is to *reduce the annual business impact of network downtime and slowdown on the productivity of the organization's users* — i.e., a strong "**enable the business**" message. As an added benefit, it's also a powerful way to *reduce the day-to-day burden on the operational staff*, by reducing time and improving accuracy for managing firewall policies, rules, and configurations through fact-based visibility, intelligence, integration, and automation.

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research

Bad Bots, Good Bots, and Humans: Quantifying the Risk of Bad Bots; September 2016
Firewall Sprawl: How Complexity is Adding Cost and Increasing Risk; October 2015
Network Security for Small and Mid-Size Business; September 2015
Flash Forward: Network Security in the Financial Services Sector; February 2015
Flash Forward: Networks Designed for Growth, Not for Obsolescence; September 2014
Three Ways to Harden the Security of Your Campus Network; May 2014

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.