ABERDEEN GROUP

QUANTIFYING THE VALUE OF TIME IN CYBER-THREAT DETECTION AND RESPONSE

January 2017

Aberdeen Group's analysis, based on empirical data, helps security professionals develop a business-level appreciation for the dimension of time in cyber-threat detection and response. Time is currently working in favor of the attackers — and is the critical strategic advantage that the defenders must regain.

The Stakes for Enterprises in Threat Detection and Incident Response Capabilities are Getting Higher

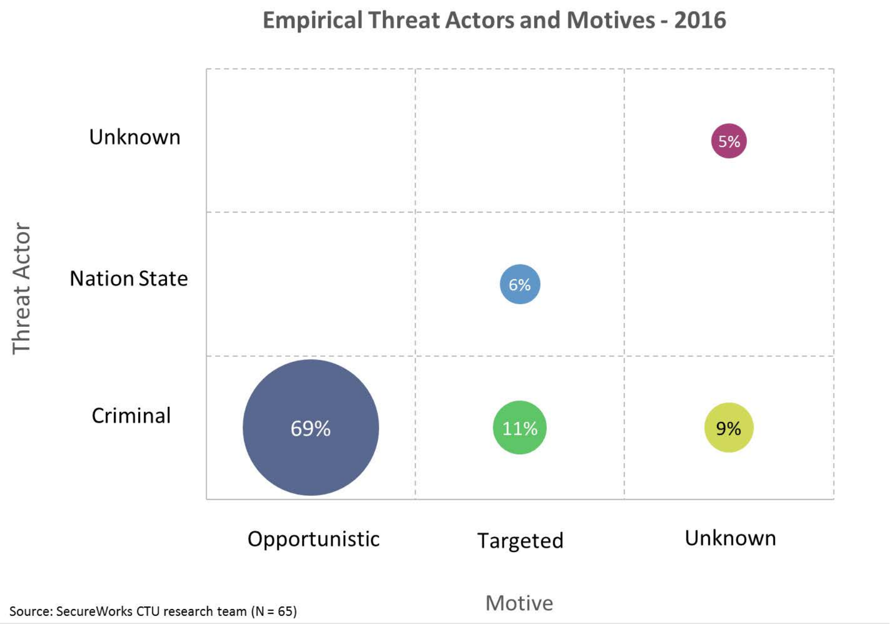
Aberdeen Group's analysis of more than 60 successful cyber-attacks in 2016 — based on empirical data provided by the SecureWorks Counter Threat Unit (CTU) research team — shows solid evidence that the stakes for enterprises are increasing (see Figure 1):

- ➔ Just under 70% of these successful cyber attacks continue to be cyber criminals, acting *opportunistically*.
- ➔ In at least one out of every six successful cyber attacks, however, enterprises were specifically *targeted* — either by cyber criminals or by a nation state.

These findings reveal that merely keeping up with the growth and complexity of the technical **threat landscape** and **vulnerability landscape** is no longer enough. Going forward, what matters most may be identifying and responding to the *singular* threat actor that has *specifically targeted* your organization.

In at least one out of every six successful cyber-attacks in 2016, enterprises were specifically targeted — either by cyber criminals or by a nation state.

Figure 1: Empirical Threat Actors and Motives - 2016



Source: Based on data from SecureWorks Counter Threat Unit (CTU) research team; Aberdeen Group, December 2016

In This Rapidly Evolving Context, Third Party Threat Detection and Incident Response Plays an Increasingly Important Role

Threat detection and incident response are clearly important — but is your organization really better off “going it alone” in these areas? That is, are enterprise investments in building these capabilities in-house the most effective approach?

➔ Related Research: *The State of SMB Security Risks: Why Most SMBs are Looking to MSSPs*

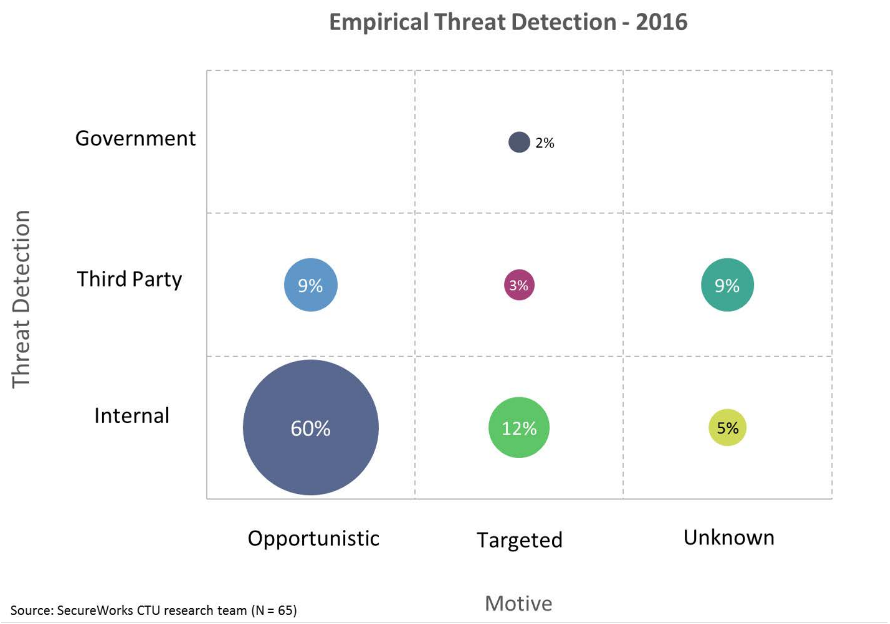
As Aberdeen noted in *The State of SMB Security Risks: Why Most SMBs are Looking to MSSPs* (December 2016), specialized third-party service providers have the *focus*, *expertise*, and *visibility across multiple enterprise subscribers* necessary to help detect and respond to advanced cyber security threats — in addition to opportunistic, commodity threats — more effectively than most enterprises are able to on their own.

In the SecureWorks CTU research team dataset, for example, third parties detected:

- 13% of *opportunistic* threats
- 18% of *targeted* threats
- 64% of threats with *unknown* motives

The empirical data also makes it extremely clear that enterprises cannot rely solely on *government* sources for detecting advanced threats (see Figure 2). Realistically, the strategic choices are to attempt to do it yourself, or to leverage the expertise of specialized third-party service providers.

Figure 2: Empirical Threat Detection - 2016



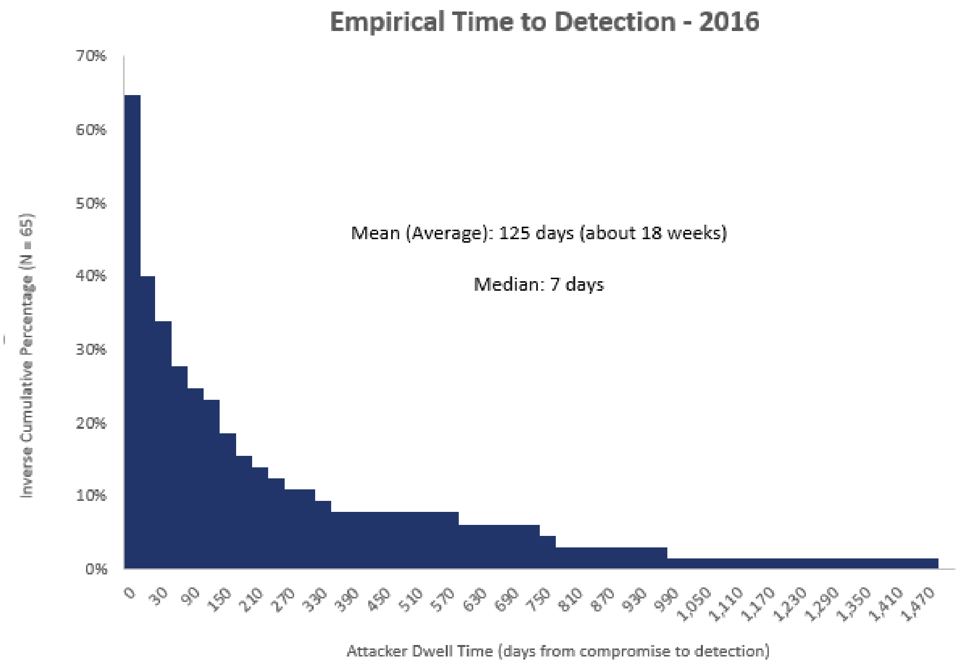
Source: SecureWorks CTU research team (N = 65)

Source: Based on data from SecureWorks Counter Threat Unit (CTU) research team; Aberdeen Group, December 2016

Appreciating the Value of Time in Threat Detection and Incident Response: Empirical Attacker Dwell Times in 2016

The empirical data from SecureWorks CTU research team provides invaluable insights into how the dimension of **time** is currently working in favor of the attackers. Figure 3 depicts the distribution of time, in days, from *compromise* to *detection* for more than 60 successful cyber-attacks (Figure 3).

Figure 3: Time to Detect and Respond Currently Favors the Attackers



Source: SecureWorks CTU research team (N = 65)

Source: Based on data from SecureWorks Counter Threat Unit (CTU) research team; Aberdeen Group, December 2016

In half of the successful cyber-attacks, detection and response by the defenders took a week or less — but in the other half, detection and response took up to *four years.*

Readers should make special note that the **mean** (*average*) for this distribution is **125 days**, while the **median** (the point at which half of the attacker dwell times are above, and half are below) is just **seven days**. What this means is that in half of the successful cyber-attacks, detection and response by the defenders took a week or less — but in the other half, detection and response took up to *four years*. This is the “long tail” of cyber security risk that is so important for security professionals to understand and communicate to the business decision-makers, to help them make a better business decision regarding whether to *accept it*, *transfer it*, or take steps to *manage it to an acceptable level*.

The Timeline of the Attackers Sets the Bar for the Defenders

Properly defined, **risk** is always expressed as a function of both *likelihood*, and *business impact*: how **likely** is it for a successful cyber-attack to take place, and what is the **business impact** of a successful cyber-attack if it actually does occur?

For the defenders, improvements in the dimension of time can help with both sides of the risk equation:

- ➔ If defenders can increase their ability to **detect**, they can reduce the *likelihood* aspect of risk
- ➔ If defenders can significantly **shorten the time to detect, respond, and recover,** they can significantly reduce the *business impact* aspect of risk

In a simplified description of the typical **attack lifecycle**, attackers *identify vulnerabilities* by doing reconnaissance of the target organization's networks, systems, and applications; *implement* and *execute* the exploits to selected vulnerabilities; and sometimes *automate* the exploits to run at scale. Additionally, attackers may also *modify* the exploits as the target organization happens to identify and eliminate the underlying vulnerabilities, staying one step ahead of the defenders.

From the organization's perspective, a simplified description of the **detection and response lifecycle** is to *identify anomalous behavior* that signifies a potential attack, followed by *assessment*, *containment*, and *remediation* of the incident, and ultimately by the *restoration* of the infrastructure to its pre-incident state. In the worst-case scenario, the organization identifies all anomalous behavior only after exploits are already being run at full scale. In the best-case scenario, the organization identifies all anomalous behavior when the attacker is doing their initial reconnaissance.

Attack lifecycle:

- Identify vulnerabilities (i.e., reconnaissance of enterprise networks, systems, and applications)
- Implement exploits
- Execute exploits
- Automate exploits (i.e., run at scale)
- Modify exploits (e.g., adapt as vulnerabilities are identified and eliminated by the defenders)

Detection and Response lifecycle:

- Identify anomalous behavior
- Assess incidents
- Contain incidents
- Remediate incidents
- Implement additional countermeasures, as appropriate

Example: Quantifying the Risk of a Data Breach

To quantify the value of time in threat detection and incident response, Aberdeen has developed a simple **Monte Carlo model** that provides invaluable insights into the annualized business impact of a **data breach** as a function of *industry*, the *number of data records compromised*, and the status quo in terms of *dwell time*. For the private sector (across all industries), based on a compromise of 1M to 10M records:

- ➔ There's a **90% likelihood** that a data breach will result in an annualized business impact of **more than $0** (i.e., there will almost certainly be at least *some* cost associated with compromised data)
- ➔ There's a **10% likelihood** that a data breach will result in an annualized business impact of **more than $6M**
- ➔ The **median** business impact of a data breach, given current capabilities for detection, response, and recovery, is **about $1.3M**

Note that this approach to analysis expresses the risk of a data breach properly, in terms of both likelihood and business impact — because by definition, risks involve an inherent *uncertainty*. The likelihood and business impact that security professionals need to advise their respective business decision-makers about are *not certain*. If we knew with certainty what was going to happen and how big an impact it would have, it wouldn't be a **risk** at all – it would be a **fact**!

Qualitatively, it's straightforward to make the point that faster detection and response capabilities would result in lower business impact from a successful data breach — especially if the attack can be detected and contained before data exfiltration begins.

Quantitatively, we can make an informed estimate for how faster detection and response capabilities would reduce the business impact of a data breach. For example, the simplest premise would

Monte Carlo Models and Risk

In a **Monte Carlo** analysis, each variable in a calculation is expressed as a *range* (lower bound, upper bound) and a *shape* (probability distribution) — as opposed to as a single, static value.

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.

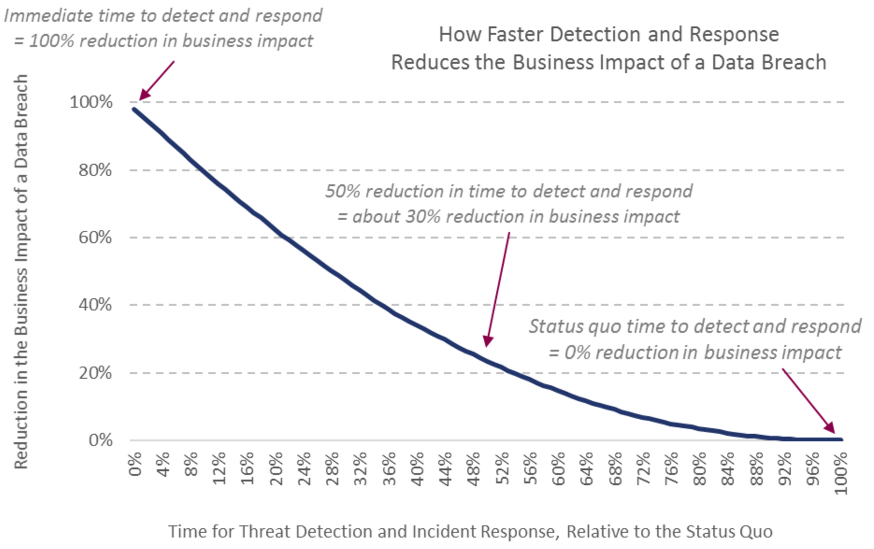
In doing so, the result is also expressed as a range and distribution — as opposed to a single, static, misleading value such as "the average cost of a data breach is $201 per record."

Most importantly, the result can then be represented in terms of both *how likely* and *how much* — i.e., in terms of **risk**, as risk is properly defined.

be that **the faster a data breach is detected, the less business impact it has**, i.e., *twice as fast, half the impact* (Figure 4).

In Aberdeen's analysis, a 50% reduction in the time to detect and respond to a data breach, compared to the status quo, reduces the annualized business impact by about 30%.

Figure 4: Faster Detection and Response Reduces the Business Impact of a Data Breach



Source: Monte Carlo analysis; Aberdeen Group, January 2017

In Aberdeen's view, it seems most reasonable to assume that the business impact from a data breach is greatest at the *beginning* of the exploit (when records are first compromised) — in which case detecting it twice as fast would actually cut the business impact by *less* than half. Incorporating this assumption into its Monte Carlo model, it turns out that *twice as fast translates to about 30% less business impact* (see Figure 4):

- ➔ Under the status quo time to detect and respond, the annualized business impact of a data breach is as described above (i.e., a median of $1.3M, with an 80% confidence interval of between $0 and $6M)

- Given a **50% reduction in the time to detect and respond**, the annualized business impact of a data breach is reduced by **about 30%**

- If the time to detect and respond were immediate, the annualized business impact of a data breach is reduced by 100% (i.e., the breach is prevented, and the data is not compromised)

Aberdeen plans to continue developing this aspect of its analysis, as additional empirical data on the factor of time as it relates to total business impact becomes available.

Summary and Key Takeaways

- Aberdeen Group's analysis, based on empirical data provided by SecureWorks CTU research team Research Team, helps security professionals to develop a business-level appreciation for the dimension of **time** in threat detection and incident response. Time is currently working in favor of the attackers — and is the critical strategic advantage that the defenders must regain.

- In Aberdeen's analysis, a 50% reduction in the time to detect and respond to a data breach, compared to the status quo, reduces the annualized business impact by about 30%.

- By quantifying the economic value of time in these areas, Aberdeen's analysis helps to validate the value proposition for enterprises to subscribe to third-party threat detection and incident response services.

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-agnostic 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.