WHITE PAPER

iSIGHTPARTNERS℠

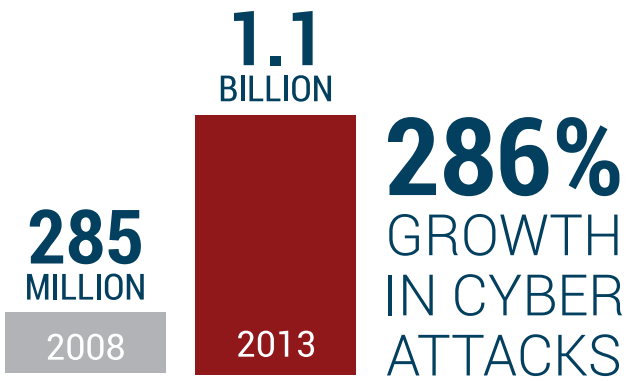
DECISION ADVANTAGE

The Benefits of Quality Intelligence on Decision Advantage Within the Cyber Security Industry

TEL 214.731.4585 | ISIGHTPARTNERS.COM

Dallas, TX • Chantilly, VA • Amsterdam, The Netherlands • Beijing, China • Sao Paulo, Brazil • Pune, India • Kiev, Ukraine • Seoul, Korea

Information security is evolving. Between 2008 and 2013, the number of records compromised by cyber attacks grew 286%, from 285 million to 1.1 billion (Verizon, 2013). These attacks are increasing in frequency and complexity to the point that the classic method of approaching information security will soon be completely antiquated. The standard methodologies of cyber security: intrusion detection, intrusion prevention and vulnerability scanning are quickly becoming archaic as intrusion tactics grow more and more complex (McMillan, 2012).



It is now the purpose of information security leaders to find and embrace new strategies while creating a model for information security that will, efficiently and effectively, guide enterprises towards decisions that positively affect their security posture while avoiding unnecessary risks and spending. The information security industry is embarking on what should be considered Cyber 2.0, a new era of information security that needs to be approached with new methods. Cyber 2.0 will focus on intelligence-led, strategic cyber security instead of relying on the current methods. These current methods are reactionary at best and lack decision advantage, defined as the "circumstances or factors that place one in a favorable position in relation to the judgment associated with coming to a conclusion or determination" (Aftergood, 2009).

> "circumstances or factors that place one in a favorable position in relation to the judgment associated with coming to a conclusion or determination."

Historically, in military strategy, decision advantage has been gained through increased intelligence and better methods of intelligence gathering. There are both real life examples of the benefits of actionable intelligence on decision-making and scholarly research quantifying those benefits. It is because of the overwhelming evidence on the advantages of intelligence within traditional strategy that cyber security is, slowly, warming to the concept of intelligence-led strategies. As the old, reactionary methods of cyber security become more and more fruitless, infor-

"How can any man say what he should do himself if he is ignorant about what his adversary is about?" *- Baron Antoine-Henri Jomini*

mation security teams will be forced to find better security tactics that create decision advantage while limiting risk and maximizing resources. Just as in other strategic fields, decision advantage in cyber security will be gained, not from increased spending or progressions in technology (although these are important factors to consider), but from deep, actionable intelligence.

Many industries, cyber security included, consider decision-making not as a scientific, definable theory but as a necessary act left to the discretion of a trusted few. Far fewer ever consider the decision-making process as one that can be improved or corrected. It is this fundamental lack of comprehension of decision-making theory that leaves so many enterprises struggling with the process, inflexible strategy and in dire need of a new perspective. The goal of any industry, when presented with a decision point, *should be to create a decision advantage*. As stated previously, the theory of decision advantage deals with the circumstances or factors that lead to an ideal state for decision-makers. Any element that creates greater decision advantage should be considered as a benefit to decision makers, particularly within the business world where better decisions can be measurably linked to a better return on investment, less wasted resources and a more streamlined business model. This applies also to the cyber security industry where, because of growing complexity and limited resources, wasting those resources has become a serious problem.

The goal of any industry, when presented with decisions that must be made, should be to create decision advantage.

So if decision advantage is so valuable for the information security industry, why has it not been implemented? It is a simple matter of growing complexity. When the industry was less developed and there were fewer actors, methods and technologies in place, breaches had neither the frequency nor the impact that they do today. As the industry evolved, the threats evolved as well, while the methods of detection and response have stayed essentially the same. Many enterprises still do not act strategically when faced with cyber security incidents, instead choosing to react to breaches that have already happened or boost security across the board with no real understanding of the threat environment. If the in-

"The value of intelligence can go largely unrecognized until the consequences of ignoring or misunderstanding threats lead to decisions being made in ignorance to or without regard to available threat information that can lead to catastrophic security (not intelligence) failures." *- Andrew Miller*

formation security industry accepts that decision advantage is crucial to cyber security, then the only factor left is to determine how to best create that decision advantage.

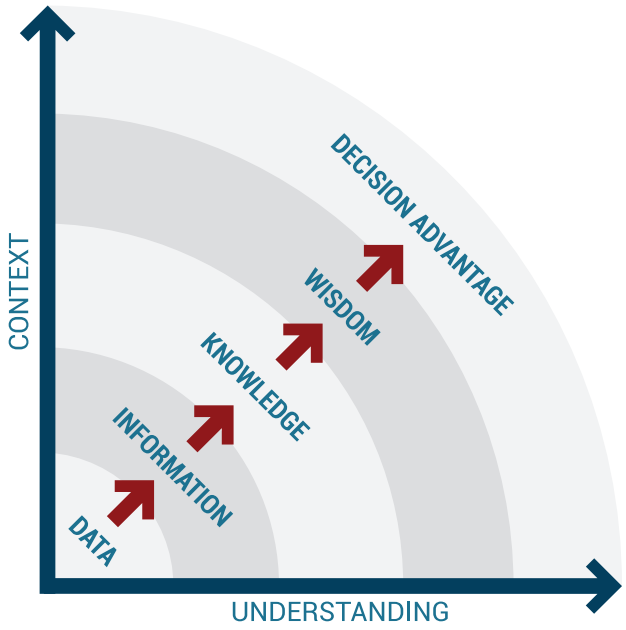
Intelligence has a longstanding history of creating value within tactical industries. It's American military roots date back as long as the nation itself, being utilized throughout the Revolutionary War, the War of 1812 and every significant battle since (Jensen, McElreath & Graves, 2013). For more modern examples, the World War II battles of Midway and Crete are often cited to illustrate the benefits of quality intelligence. These battles allow us to objectively analyze the advantage of quality intelligence and the difference it makes on decision advantage because of their many similarities. Both were instances of Axis aggression and both attacks were predicted with relative accuracy, at Midway by the U.S. Navy and at Crete by British forces. While both battles were anticipated similarly by intelligence teams, the confidence in the quality of intelligence was dramatically different. It was the quality of intelligence, and the way it was provided, at Midway that resolved the US Navy's dilemma and allowed it to adequately meet the Japanese attack while the lack of quality intelligence and poor transmission provided at Crete kept the British commander from using adequate force against the German attackers (Piotrowicz, 2011). In other words, *in the battle of Midway, it was the quality of the intelligence that provided the decision advantage necessary for victory*.

It was after World War II that President Truman realized that the intelligence framework that existed up to that point was insufficient to deal with future intelligence needs, and created both the National Security Council and the office of Director of Intelligence. Considering the rapid advancement in warfare tactics and technologies, and the growing complexity of military models, it made sense that intelligence became a priority for post WWII America. However, alongside those touting the new intelligence framework and its offerings, were deniers that claimed that resources spent on intelligence were being wasted on what essentially amounted to a strategic fad (Jensen, McElreath & Graves, 2013). Many of the problems that deniers have had with intelligence-led strategies were built upon a basic misunderstanding of the purpose of intelligence. A scholar in the field of homeland security intelligence, a field that shares many strategic pain points with that of information security, Captain Andrew D. Miller states that the purpose of intelligence is not to acquire threat data, draft reports or predict adversary activity. Instead, he believes that intelligence should "facilitate decision advantage for leaders and practitioners" (Miller, 2004). In other words, the purpose of intelligence is not to know, but to inform knowledgeable choices. We can see

> "the purpose of intelligence is not to acquire threat data, draft reports or predict adversary activity... but to facilitate decision advantage for leaders and practitioners."

then that intelligence has no other goal than to create decision advantage, to provide better decision-making abilities to the leaders and practitioners within the industry it serves. Despite scholarly claims that decision advantage can be gained from deeper intelligence, there still remains doubt in the minds of many CEOs, CISOs, CTOs, and others charged with the creation of high-level cyber security strategies.

The DIKW model depicts a hierarchy of understanding designed to show the differences between types of comprehension, the links between these types and the path from one type to the next.



The model seeks to explain that data turns to information, information to knowledge and knowledge to wisdom. This model, created in part by Chinese-American geographer Yi-Fu Tuan and sociologist-historian Daniel Bell and augmented by others since its inception, has recently been enhanced by Eric McMillan. McMillan argues that intelligence serves as the impetus for the entire DIKW model. (McMillan, 2013) According to McMillan, data evolves up the DIKW scale, from data through wisdom, driven by the techniques, methodologies and tools traditionally utilized in intelligence analysis. If we accept that intelligence acts as the impetus to make progress along the DIKW scale, It could be argued that, concurrently, the level of decision advantage rises parallel to that of understanding. As one rises through the levels of information intelligence, one also rises through tiered layers of decision advantage from the initial, data driven decision tier all the way to "wise decisions," or those assisted by wisdom.

When the DIKW model is applied to decision-making, decisions at the first level, which rely simply on raw data, should be considered akin to reactionary decisions. These are fueled by insufficient knowledge and powered, not by wisdom, but by instinct or habit. At the information stage of the DIKW model we see decisions becoming informed, at the knowledge stage decisions become knowledgeable and at the wisdom stage truly wise decisions can be made. Given McMillan's compelling argument that the DIKW scale is, in fact powered by intelligence at every stage, it is not difficult to make the connection from information to informed decisions. It is this model of decision-making, centered around informed decisions and powered by intelligence, that should be at the heart of decision-making strategy, particularly in the cyber security industry where the repercussions of poor security can have far reaching consequences and attacks like Titan Rain, 50

days of Lulz and Ghostnet have shown the real power of intrusion. (Keating, 2012)

> Titan Rain, 50 days of Lulz and Ghostnet have shown the real power of intrusion.

So if the benefits of intelligence-led decision advantage are self-evident, how can this knowledge best be applied to the cyber security industry? Considering that many enterprises are still utilizing a rudimentary method of intrusion detection, intrusion prevention and vulnerability scanning, simply adding intelligence to this mixture would not provide the effectiveness that a total overhaul would. Information security teams do not need another tactic added for their arsenal, they need a new arsenal, built from the ground up and centered around intelligence-led decision advantage. This is the core concept behind Cyber 2.0 and intelligence-led security, that decision advantage is gained as one progresses up the DIKW scale, from data to wisdom. It will only be when the cyber security industry creates decision advantage regarding the threats, actors and methods it is facing that a valuable, holistic approach to information security will be found. As previously stated, just as in warfare, decision advantage in cyber security will be gained, not from simply increasing resources, but from intelligence designed and gathered for the sole purpose of assisting the decision-making process.

At iSIGHT Partners, we've developed the infrastructure to ensure decision advantage. We've built an extensive security analyst that spans 16 countries and 24 languages in order to provide deep, contextual intelligence on the cyber threat environments of Fortune 100 companies and governments across the globe. By utilizing iSIGHT Partners' proprietary intelligence, enterprises can ensure that their assets, as well as the personally identifiable information of their customers, remain secure and confidential. At iSIGHT Partners, we pride ourselves on the quality of our intelligence, the decision advantage it provides and our commitment to the tenets of Cyber 2.0.

CURRENT METHODS IN CYBER SECURITY

Intrusion Detection - the act of discovering attempts to compromise a network or database resource.

Intrusion Prevention - a proactive method of identifying and responding to potential threats.

Vulnerability Scan - searches for weaknesses in a system and reports possible exposures.

Aftergood, S. (2008, September 17). [Web log message].
Retrieved from http://blogs.fas.org/secrecy/2008/09/osint_secrecy/

Jensen, C. J. I., McElreath, D. H., & Graves, M. (2013)
Introduction to intelligence studies. Boca Raton Fl. : CRC Press.

Keating, J. E. (2012, February 29th). The 10 worst cyberattacks.
Retrieved from http://bangordailynews.com/2012/02/29/news/nation/the-10-worst-cyberattacks/

McMillan, E. (2012). Promoting the use of intelligence and intelligence analysis as complementary components to enhance situation awareness in cyber security. (Master's thesis, Pennsylvania State University) Retrieved from https://etda.libraries.psu.edu/paper/14625/

McMillan, E. and Michael T. "An Alternative Framework for Research on Situational Awareness in Computer Network Defense." Situational Awareness in Computer Network Defense: Principles, Methods and Applications. IGI Global, 2012. 71-85. Web. 14 Aug. 2013.
doi:10.4018/978-1-4666-0104-8.ch005

Miller, A. (2008). Homeland security intelligence: To what end? (Master's thesis, Excelsior College).

Piotrowicz, E. J. (2011). The battle for intelligence: How a new understanding of intelligence illuminates victory and defeat in world war ii. (Master's thesis, Georgetown University) Retrieved from https://repository.library.georgetown.edu/bitstream/handle/10822/553559/piotrowiczEdward.pdf

Simon, H. (1978) "Rational Decision-Making in Business Organizations," Nobel Lectures, Economics 1969–1980, Singapore: World Scientific Publishing.

Verizon (2013). Verizon 2013 data breach investigations report.
Retrieved from http://www.verizonenterprise.com/DBIR/2013/

WHITE PAPER

About iSIGHT Partners

iSIGHT Partners is a global cyber threat intelligence firm that delivers actionable intelligence products and services to leading enterprises in business and government. With a global network of security analysts and geographic research and analysis centers in Washington DC, The Netherlands, Brazil, Ukraine, India and China, iSIGHT Partners is uniquely positioned to monitor and mine the cyber threat ecosystem and deliver proprietary intelligence products and services specific to the threats its clients face.

 | TEL 214.731.4585 | ISIGHTPARTNERS.COM | INFO@ISIGHTPARTNERS.COM

Dallas, TX • Chantilly, VA • Amsterdam, The Netherlands • Beijing, China • Sao Paulo, Brazil • Pune, India • Kiev, Ukraine • Seoul, Korea