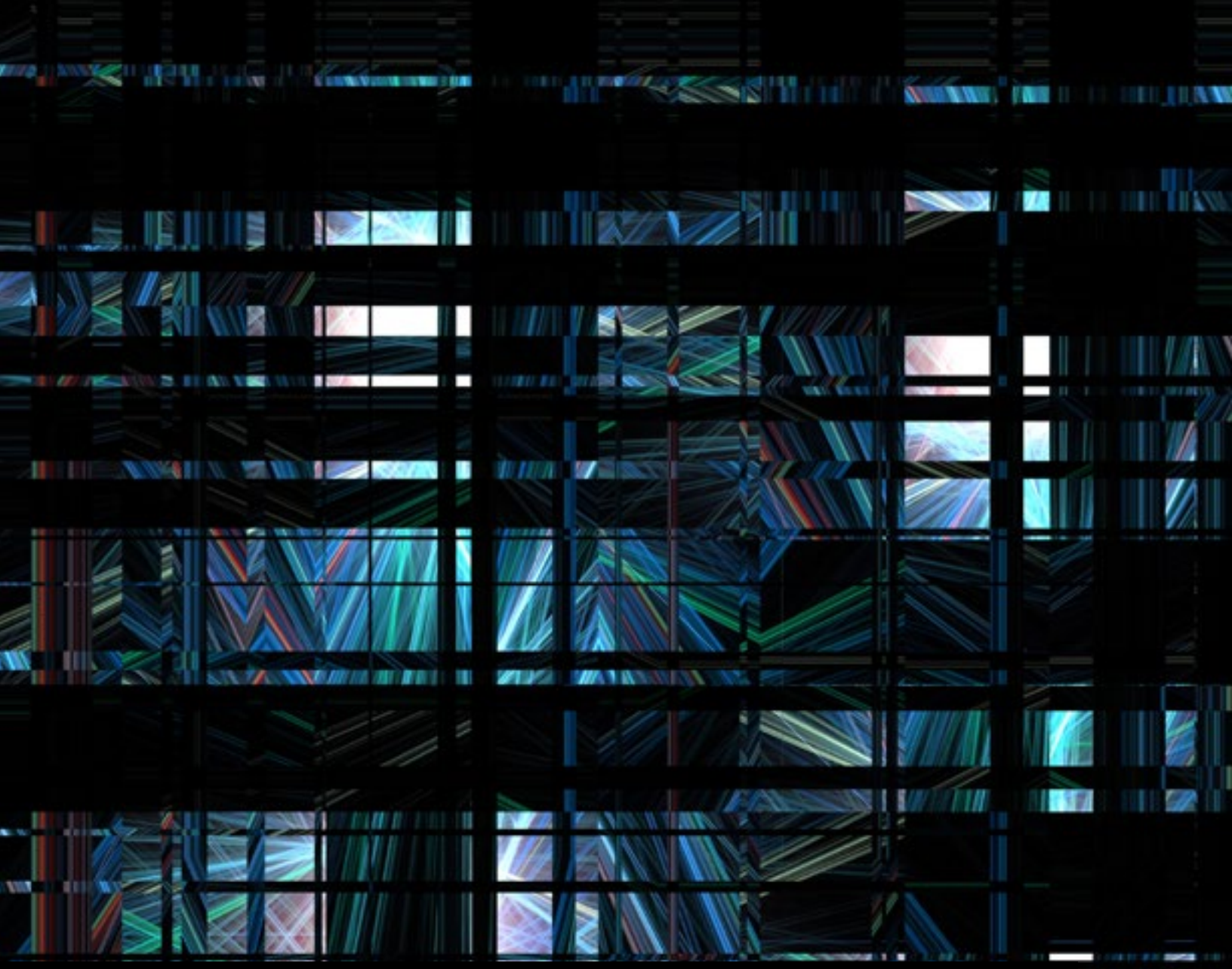


Economics of Insecurity

By Malcolm Harkins, Chief Security & Trust Officer

CYLANCE

Introduction

The information security field is economically inefficient. This is both good and bad. Bad, because it means billions of dollars are squandered on solutions which offer their buyers sub-optimal returns. Good, because the opportunities exist to operate more efficiently and thereby improve the quality of life for everyone.

This paper will examine how we know economic inefficiencies exist and why the industry seems unwilling to address them. By understanding these issues, companies will be better able to select effective IT security solutions that align with their business mission. Readers will also gain insight into how misplaced trust can lead to contradictory market reactions.

Signs of Economic Inefficiency

Economic efficiency is defined as:

> An economic state in which every resource is optimally allocated to serve each individual or entity in the best way while minimizing waste and inefficiency[1].

It is worth noting that the welfare (or quality of life) of populations in an economy is directly impacted by the efficiency of resource allocation. Peak efficiency is reached when the available resources could not possibly be allocated in a more efficient manner.

Keeping this in mind, it's worth examining the current state of information security. *Forbes Magazine* reports that companies will spend an estimated $93 billion on information security in 2018[2]. This represents a 14% increase over the $71.4 billion that companies spent in 2014[3]. During this same time period, we have witnessed devastating cyberattacks against JPMorgan Chase, Home Depot, Equifax, and Yahoo, just to name a few. Global threats like WannaCry and Petya have dominated headlines while advanced persistent threat actors have taken down power grids in Ukraine.

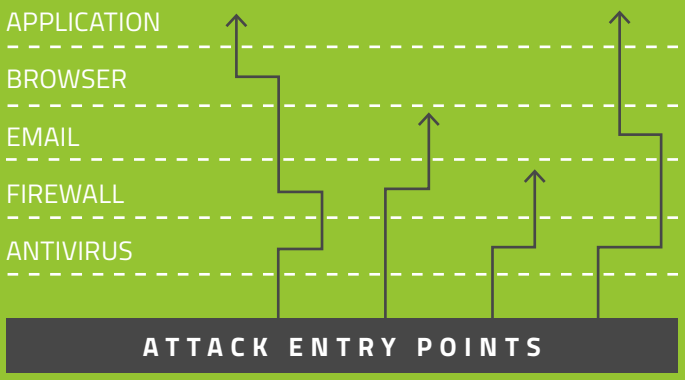
Does this sound like an industry that is delivering peak efficiency to its customers?

The Center for Strategic and International Studies has been tracking significant cyber incidents since 2006. They define a significant attack as one which targets "government agencies, defense and high-tech companies, or economic crimes with losses of more than a million dollars"[4]. Their research indicates significant cyberattacks have increased 230% since 2014. In other words, companies are paying 14% more to stop a problem that has grown 230% worse over the last four years.

This is a telltale sign of economic inefficiency.

Root Cause of Inefficiency

The primary cause of economic inefficiency is the misallocation of resources. To understand how the information security sector has traditionally mishandled resources, we must examine how the industry develops solutions. Antivirus software and other security solutions evolve by crafting responses to new threats. Each new solution adds a layer of protection to the last.



Old Industry Model

While this method of responding to threats is completely understandable, it is not particularly efficient. Every layer of protection may require additional resources. Following a pattern of erecting new defenses to address emerging threats ultimately leaves security solutions top heavy and demanding on resources.

The end result is predictable inefficiency. Every minute dedicated to learning new systems, every clock cycle spent processing additional security data, is one diverted away from the core business. Multiple layers of new protections built upon legacy solutions introduce control frictions into the environment. This directly impacts productivity, which results in inefficiency.

Cylance® Prevention Model

Who Profits from Insecure Computing?

The WannaCry global ransomware attack made headlines on May 12, 2017. Three days later, Reuters ran a story titled "Cyber security stocks rise in wake of global 'ransomware' attack"[5]. A month later, the Petya (later deemed NotPetya) malware attacks hit Ukraine before spreading to sixty-four other countries. NASDAQ reported "Cybersecurity Stocks Shoot Up on Petya Ransomware Attack"[6] two days after the initial breach. These malware-driven market gains were reflected both in the stocks of individual antivirus (AV) companies and ETFs broadly tracking the information security sector.

Though it seems counter-intuitive, information security companies profit from security breaches. An optimist might assume these stock increases reflect an influx of unprotected business owners rushing to secure their systems during a malware outbreak. If that were the case for WannaCry in May 2017, what explains the same market reaction occurring when the Petya attack happens in June?

An industry built upon providing secure computing should not profit from failures. Consider the economic ramifications that occurred when mad cow disease appeared in the U.S. American ranchers did not reap higher prices for cattle. On the contrary, the U.S. beef industry lost almost $11 Billion[7] over three years. Considerable losses in the wake of a public failure is a common market reaction whether a company sells automobiles, fast food, or smartphones. Yet the information security sector has proven an exception to the rule, largely because of misplaced public trust.

"The reactive nature of legacy AV protection has led to a proliferation of inefficient, ineffective, solutions. Today's businesses require lightweight, proactive solutions that focus on preventing breaches instead of responding to them."

Misplaced Trust

Trust derives from two foundational traits: competence and character. Competence engenders trust by demonstrating capability and delivering results. Character earns trust by displaying positive intent and integrity. The public trusts information security companies to protect them from malware. This is clear by the positive market reaction AV companies enjoy during outbreaks of global malware. It is not clear that this trust is deserved.

Competence — It is difficult to claim the information security industry has demonstrated increased competence over time. Every year seems to bring more serious security compromises than the last. In response, people throw more money at the very industry which failed to protect them. This may be followed by the AV companies offering a slew of new products or services. These after-the-fact solutions may cost more money and add more control friction to the IT environment.

Character — The following comment regarding security breaches was made at the ISSA CISO panel in Los Angeles in May 2017:

"Accept it… they are going to get in."

Unfortunately, the statement reflects a core belief repeated by many in information security. Yet, the goal of IT security is not to reduce intrusions, it is to stop them. Therefore, it is legitimate to question the intent of companies who operate under the premise that cyberthreats cannot be stopped.

Business Alignment

Businesses should make sure their security provider's goals are aligned with their own. Are the people selling business security solutions concerned with the overall efficiency of the company? Or are the vendors pushing inefficient, multi-layered, patchwork products that function under the assumption that some breaches are inevitable?

The reactive nature of legacy AV protection has led to a proliferation of inefficient, ineffective, solutions. Today's businesses require lightweight, proactive solutions that focus on preventing breaches instead of responding to them.

To further illustrate the point: the old model of information security offers to sell your business fire engines, hoses,

hydrants, and ladders in the event of an arson. A company aligned with your business would offer a more proactive, less resource-heavy solution. They might build your business from fire-retardant materials, in a safe neighborhood, and install monitors to ensure no arsonist enters the premises undetected.

Conclusion

The reactive nature of information security has led to the creation of multi-layered, inefficient, and ineffective solutions. Security providers have embraced a philosophy of inevitable data breaches which fosters a culture of mediocrity and apathy. Misplaced public trust allows the AV sector to fail while avoiding the downside of standard market forces. Since IT security companies profit from the current situation, they have great incentive and many reasons *not* to change.

The future of successful information security requires the selection of proactive, preventative, lightweight solutions that align with the buyer's business mission. They should introduce a minimum amount of control friction into the IT environment, and their goal should be 100% threat prevention, not an endless cycle of erecting new defenses over the broken remains of the last.

For the last four years, the information security sector has been charging more for less. Until or unless the market's understanding of the security industry changes, this trend is likely to continue.

Endnotes

[1] Economic Efficiency, (Investopedia, 2018)

[2] Gartner Predicts Information Security Spending To Reach $93 Billion In 2018, (Forbes, 2017)

[3] Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020, (Forbes, 2015)

[4] Significant Cyber Incidents, (CSIS, 2018)

[5] Cyber security stocks rise in wake of global 'ransomware' attack, (Reuters, 2017)

[6] Cybersecurity Stocks Shoot Up on Petya Ransomware Attack, (NASDAQ, 2017)

[7] Mad-cow ban cost U.S. $11 billion in beef exports, (Reuters 2008)

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

CYLANCE

20180125-0108