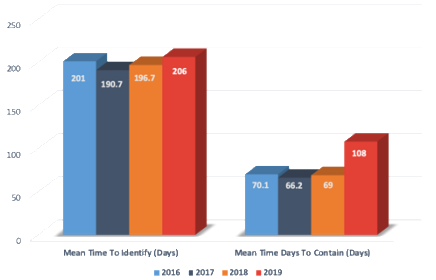
Cyturus™
Something Different Something Better

Examining the Cybersecurity Quandary

Robert Hill, CISSP
Cyturus CISO

January 2, 2020

In 2019 organizations spent over $120 billion on cybersecurity tools, products, and services and yet we witnessed an 11% increase in attacks[1], a 4.9% increase in both meantime to identify and meantime to contain attacks[2], as well as an 1.5% increase in the average cost of damages caused by these attacks[3]. This whitepaper seeks to examine the root causes and define the insanity of repeating behaviors from which there seems to be no measurable improvement. We call this the *Cybersecurity Quandary*.



Source: Ponemon Institute - 2016, 2017, 2018, 2019 Breach Report data

The first step in disrupting this repetitive cycle starts with the acknowledgement that the established belief, which implies cybersecurity is an IT problem to be solved by the implementation of specific and defined technology controls, is flawed as evidenced by the increasing frequency of successful attacks. Despite being surrounded by evidence to the contrary, business still holds on to a fundamental belief in a magic bullet for enabling cybersecurity maturity.

The business wants to believe there is mysterious voodoo which can be performed by the IT team enabling the protection of their business assets and interests from malicious harm. For its part in this fallacy, IT has perpetuated this belief through the lack of transparency, increasingly stringent controls impacting the business's abilities to deliver services, and requests for budget increases while accepting and assuming the responsibility to 'solve' the cybersecurity crisis. Gartner published a profound thought in 2016 when they said "*many organizations falsely equate IT security spending with maturity*. "

There exists a commonly held misconception that if the business throws enough money at a problem, a solution can be bought. This is simply not the case with cybersecurity. Let's explore why.

We must examine the history of IT to understand how we arrived at the *Cybersecurity is an IT problem* belief. The first computers were designed to provide efficiency and increase accuracy when problem solving. A complex problem could be loaded into a machine and a consistent answer was swiftly delivered upon request. The accuracy of the answer depended upon the programming supplying the answer, but the answer provided was faster and more consistently delivered than the same complex problem being solved by a human. From that point forward, when the business presented a problem, IT developed a solution. The need to access and share vast amounts of information started with the military and then grew into colleges and universities and finally into businesses and private individuals. The internet was born and has since grown into an entity we now rely on for many aspects of our business and personal lives. Business needed to disseminate data and information to various entities quickly, so IT delivered the electronic mail (e-mail) solution. Business wanted to reduce their reliance and associated expenses for private data centers, so IT delivered Cloud as a solution. Business wanted to expedite service delivery, so IT delivered SaaS as a solution. We could continue with more examples, but you see the emergence of a pattern. Historically, IT solves business' problems.

DEFINITION:
Cybersecurity is the body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access.

Before we move on, let's define the term Cybersecurity for the purposes of this whitepaper to assist when identifying the context of the terms use as we progress forward. Cybersecurity is defined as the body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access.

Now that we have defined cybersecurity as encompassing the technology and the activities associated with protecting business assets, including data, from not only attacks but also from damage and unauthorized access, we need to discuss the requirements for cybersecurity. These requirements are the fundamentals for cybersecurity effectiveness known as the CIA – *Confidentiality, Integrity*, and *Availability*.

- Confidentiality refers to the confidentiality of business data, confidentiality of intellectual property, and the confidentiality of client information to reduce exposure.
- Integrity implies the intent to minimize harm to business data or to the business reputation.
- Availability refers to the loss of business data or access to the business data.

As viewed through the fundamentals of CIA, the effectiveness of cybersecurity is measured by minimizing the impact to the business, the business data, and the ability for the business to provide a business service to its clients. Cybersecurity is a business issue, or quite simply put, *cybersecurity is a business problem.*

As previously referenced and identified through a historical pattern, when the business has a problem, IT solves the business problem. Now we have reached the root cause of the misconception that *cybersecurity is an IT problem to which IT should provide the solution*. In actuality, cybersecurity is a business problem which can only be solved by a rational acceptance of this reality by the organization through a paradigm shift and adoption of an Enterprise Culture of Cybersecurity embraced by the business itself.

> "Cybersecurity is a business problem which can only be solved by a rational acceptance of this reality by the organization through a paradigm shift and the adoption of an Enterprise Culture of Cybersecurity embraced by the business itself."

Beyond the historical consistency of IT being the identified solution provider for business problems, there is a much deeper psychological aspect to this relationship dynamic between IT and the business. It starts with a simple cycle where the business requires cybersecurity, IT has the expectation to provide cybersecurity, and the business is expected to pay for cybersecurity. However, we are witnessing an ever-increasing number of breaches and loss of information critical to the business who inevitably blames IT which contributes to the systematic breakdown of this simple cycle. We see this breakdown most clearly in responsibility, authority for decision-making, and most importantly accountability. Post-breach we commonly observe the CISO and security team being blamed by the business, yet pre-breach we observe the same business denying tools, resources and budget increases requested by the very same security team who is now shouldering the responsibility for the negative consequences to the business.

Let's look deeper into some of the human psychology driving this conduct. One of the most famous studies into the psychology of obedience was carried out by Stanley Milgram, a psychologist at Yale University[4]. For over a decade he conducted experiments focusing on the conflict between obedience to authority and personal conscience. Milgram found people tend to obey orders from other people if they recognize their authority as morally right and/or legally based. He went on to write "The extreme willingness of adults to go to almost any lengths on the command of an authority constitutes the chief finding of the study." Milgram explained the behavior of his participants by suggesting that people have two states of behavior when they are in a social situation:

The autonomous state	People direct their own actions, and they take responsibility for the results of those actions.
The agentic state	People allow others to direct their actions and then pass off the responsibility for the consequences to the person giving the orders. In other words, they act as agents for another person's will.

Milgram suggested that two things must be in place for a person to enter the agentic state:

1. The person giving the orders is perceived as being qualified to direct other people's behavior. That is, they are seen as legitimate.

2. The person being ordered about is able to believe that the authority will accept responsibility for what happens.

Agency theory says that people will obey an authority when they believe that the authority will take responsibility for the consequences of their actions. We see this behavior in the business to IT cybersecurity relationship and have all

heard the "they told me to do it" Milgram justification. The business has an authoritative position to which the IT teams must acquiesce, but then when an incident occurs, the business is less willing to accept responsibility for the consequences. This is not to say this behavior is calculated, malicious, or even intentional. During a recent engagement, a CEO acknowledged this dynamic in a candid statement to his Director of Information Security saying: "I knew we underspent on cybersecurity." However, he continued his thought, "I did not recognize the amount of business risk we were accepting as an unseen consequence of that decision."

> "I knew we underspent on cybersecurity. I did not recognize the amount of business risk we were accepting as an unseen consequence of that decision."
> - Biopharmaceutical CEO

DEFINITION:
A finite game is played for the purpose of winning, an infinite game for the purpose of continuing the play. In a finite game, the rules are fixed until there is a winner, but in an infinite game, the rules change throughout the course of play.

Lastly, we need to explore the *infinite zero-sum* quantities presented by the engagement efforts associated with cybersecurity. We must once again define these terms to provide context for their use in this whitepaper. Let's first look at finite vs infinite engagements. A finite game is played for the sole purpose of winning. An infinite game is played for the purpose of continuing the play. In a finite game, the rules are fixed until there is a winner. Inversely, in an infinite game, the rules change throughout the course of play.

We commonly define business as an example of an infinite engagement because the only end is merger, acquisition, or bankruptcy. Business is performed with the expectation of perpetuity and with the purpose of continuing into the future. Incongruently to the infinite model, many use finite terminologies when describing business operations. They speak of winning and being first or number one. They measure successes against a finite period of time, albeit quarters or annual denotations. This idea of a winner and a set of rules are not applicable when in an infinite engagement. Cybersecurity is a true infinite engagement. *No one wins cybersecurity*. There is no finish line, no magic product that will eliminate current and future risk to the business interests, no set of controls with an automatic side effect of effectiveness and capacity, and no set of rules to which all parties adhere.

Zero-Sum is the next term to define in context to this whitepaper. A zero-sum is a mathematical representation of a situation in which each participant's gain or loss is balanced by the losses or gains of the other participant. "What is good for me is not good for you and what is good for you is not good for me."

DEFINITION:
A zero-sum is a mathematical representation of a situation in which each participant's gain or loss is balanced by the losses or gains of the other participant.

When we use these explicit terms together to define cybersecurity activities, we get ***infinite zero-sum***. This phrase characterizes the activities of the cybersecurity team as being perpetual with constant changing rules and where the best possible outcome is a consistency of balance between the malicious actors and the organizational cybersecurity team.

This concept is in direct conflict with commonly held perceptions of business. The business subscribes to the models requiring a direct and tangible relationship. If expenses are deemed too high and revenues too low, business reduces spend through lay-offs, budget reductions, or other cost savings and expects to see an

immediate reduction in expenditures and a return to a measured balance. Business wants to see direct correlation and they use terms such as Returns on Investments (ROI). Those concepts are difficult to attribute to infinite zero-sum activities. This is a root cause of many executive leaders not fully understanding the implications of decisions being made concerning cybersecurity. In cybersecurity, success is measured by what doesn't happen vs a direct correlation of the tangible. As an example, if a specific cybersecurity tool, resource, or control is not approved or implemented by the business, there may not be an immediate correlation or impact to the organization. The business then feels justified and/or validated in their decision and they become more emboldened because there were no immediate consequences. This is short-sighted thinking. The consequences may be postponed, but they *will* eventually occur because in a zero-sum scenario, balance can be shifted simply by not taking action against an opponent who never sleeps, is constantly pursuing potential weaknesses, and is financially motivated.

In this whitepaper we have explored the causes of this dichotomy between the business and the IT cybersecurity teams, but one may ask how to solve these issues and improve cybersecurity while providing quantifiable value to the business.

Every journey starts with a first step. The first step in this process is a fundamental mental shift from *Cybersecurity being an IT problem* to acknowledging *Cybersecurity is a business problem* and the business has both *actionable activities* and *accountability* associated with securing the organization. The second step is withdrawing from the established belief that implemented IT controls are the answer to cybersecurity issues. While controls serve a valid and important function, they are not a panacea and without measured effectiveness they provide little beyond checking a compliance box. Organizations must recognize and then internalize the shift toward measurable reduction of business risk. While a focus on compliance is necessary for many organizations, it should not be the only focus. Compliance alone does not equate to security maturity. A focus on threat avoidance is also necessary but does not link directly to measurable maturity. When an organization adopts a risk-based model, lack of compliance is seen as a business risk, avoiding threats is seen as risk reduction; however, they are not the only risks with focus. The proprietary Cyturus Adaptive Risk Model enables an organization to:

1. Identify Risks which could impact the delivery of business services
2. Measure those Risks against benefit, probability, and impact
3. Prioritize those Risks which have the greatest potential to impact the delivery of business services
4. Focus remediation efforts into those areas providing the greatest value in Risk reduction following a focused, calculated, and methodical roadmap for enterprise cybersecurity capacity maturation

By adopting a model that enables organizations to adapt rapidly to changing technical environments, fluctuating organizational needs and aggregating business threats, one can offset the innate inequality caused by resource limitations, unlimited malicious actors, and idealistic expectations.

Cyturus not only developed the evolutionary Adaptive Risk Model, we also pioneered an industry exclusive capability to calculate a quantifiable Cybersecurity Maturity Index (CMI) to numerically represent an organizationally measured maturity quotient. Cyturus is not only Something Different, Cyturus is Something Better.

Cyturus™
Something Different Something Better

[1] Bissell, Kelly (2019) *Ninth Annual Cost of Cybercrime Study* – Accenture.com
[2] Ponemon Institute (2019) *Cost of a Data Breach Report* – Ponemon.org
[3] Ponemon, Larry (2019) *What's New in the 2019 Cost of a Data Breach Report* -SecurityIntelligence.com
[4] McLeod, S. A. (2017) *The Milgram Shock Experiment* - simplypsychology.org