July 2019

THE RISE OF THE CYBER INDUSTRIAL COMPLEX AND EXPENSE IN DEPTH

Authored By:

Malcolm Harkins
ICIT Fellow
Former Chief Security and Trust Officer at Cylance /
Chief Security & Privacy Officer, Intel

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

The Rise of the Cyber Industrial Complex and Expense in Depth

July 2019

By Malcolm Harkins, ICIT Fellow, Former Chief Security and Trust Officer at Cylance, Former Chief Security and Privacy Officer, Intel

www.icitech.org

The Rise of the Cyber Industrial Complex and Expense in Depth

Almost 60 years ago, Dwight Eisenhower gave his indelible speech on the military industrial complex. In the speech, he talked about the need "to find essential agreement on issues of great moment, the wise resolution of which will better shape the future." He also spoke about how we should use our "power in the interest of world peace and betterment," and that to strive for less would be "unworthy." He astutely called out that "good judgment seeks not only balance, but progress" and "the lack of it eventually finds imbalance and frustration."

As I approached my 17th RSA conference at the beginning of 2019, I reflected back on Eisenhower's speech and realized more fully what I had witnessed for almost 18 years: the rise of a cyber industrial complex. Seventeen years ago, the RSA conference was attended by several thousand people, and had a few hundred sessions and vendors. This year, the conference drew an estimated 45,000 attendees to more than 550 sessions and 700 vendors, in addition to all the other unaccounted-for activities and adjacent attendees for ancillary meetings, side conferences, and the multitude of other vendors roaming around without a booth.

But even with the growth of security vendors and the attendant rise in spending, we have not delivered real progress as an industry, as evidenced by the continued exponential growth in the cyber risk cycle. Some say this is because we have historically underfunded information security; but, while that may be true, it's only a contributing factor and not the full story.

I came to the conclusion almost 10 years ago that the security industry profits from the insecurity of computing and thus, at a macro level, has no real economic incentive to solve the problem. I have written on this subject many times, spoken about it at many conferences, and even testified before the Senate Committee on Commerce and Science in 2017 on the financial motivation of the industry as it exists today. I also recently shared the economic motivations of the industry at the FTC hearing on data security in December 2018.

In 2002, in my early days running security at Intel, I drew a diagram called "The Perfect Storm of Risk." As published in my book, "Managing Risk and Information Security," the diagram (figure 1) shows how threats exploit vulnerabilities and the confluence of several other interdependent factors that can fuel this storm of risk. My role has been, and always will be, to understand these factors to the best of my abilities and properly control for the risks that could affect my organization, my customers, my shareholders, and our broader society.

"The Perfect Storm of Risk"

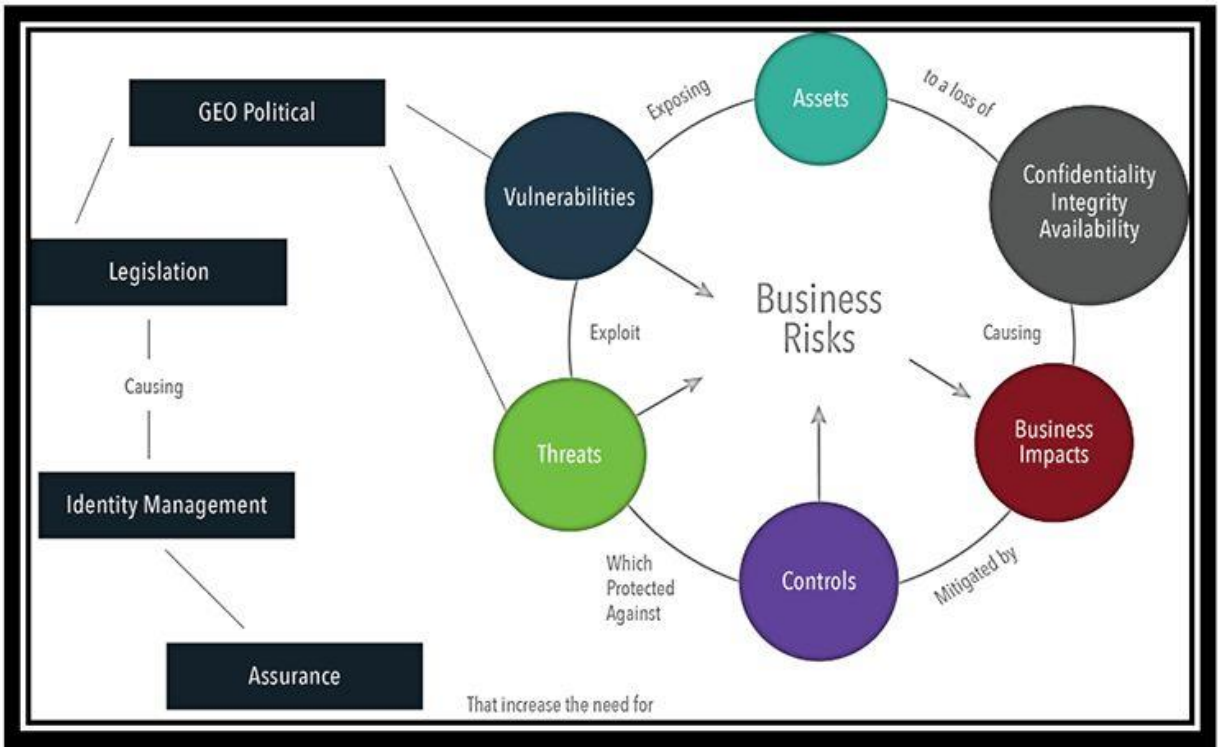


Figure 1 - Source: Managing Risk and Information Security, 2nd Edition, Malcolm Harkins

Since I first drew this diagram in 2002, I believe we have all witnessed a perfect storm of risk with full force at one time or another. The storm of risk continues to grow year after year, despite thousands of new security vendors and thousands of new capabilities sold that purport to control for these risks. We have also all witnessed a plethora of public policy discussions around cybersecurity that have called out the national security dangers we face and, in some cases, state bold initiatives to tackle such problems, only to see no real progress made to mitigate the risk.

Why is this? Why haven't we as an industry made substantive progress on managing the cyber risk cycle?

Perhaps a fundamental reason why progress hasn't been made is because of the economic incentives of the industry, as mentioned above. Eisenhower warned back in 1961 that "we must guard against the acquisition of unwarranted influence by the military industrial complex" and that "the potential disastrous rise of misplaced power exists and will persist." He warned that "public policy could itself become the captive." I believe this is manifesting today as the lack of progress toward managing cyber risk, resulting from the cyber industrial complex's lack of a proper economic incentive to solve the problem.

Looking back on my "Perfect Storm of Risk" model, I must update this timeless diagram with the hidden hand of the industry itself, which, "whether sought or unsought," has contributed to this

cycle – first by not being accountable for the controls that failed, then by pursuing a public policy agenda meant to influence legislation in the industry's favor. This not only protects the industry but also promotes compliance regimes that do little good in mitigating the real risks we face as individual citizens and as a society. The industry has taken the notion of defense in depth to manage risk and turned it into a cycle of expense in depth that generates economic waste by pervasively focusing on a reaction to risk and adding layers to mitigate failed controls, rather than having a control bias to either prevent or stop the cycle of risk as early as possible.

On March 5 at the RSA conference, I gave a talk on Expense in Depth. I described our current approaches to information security as economically inefficient. I explained the concept of total cost of controls and offered a new paradigm around managing risk, using an economic lens to get us out of the current cyber industrial complex paradigm. I explained with real-world examples how a paradigm shift in how we approach controls can not only reduce risk, but also lower the real long-term economic costs to our organizations.

WE CAN DO BETTER AT CONTROLLING FOR RISK TODAY AS WELL AS TOMMOROW

Emerging technologies, coupled with the right risk profile and control assessment frameworks, enable better risk mitigation.

In the world of cybersecurity, the most frequently asked question focuses on "who" is behind a particular attack or intrusion, and may also delve into the "why." We want to know whom the threat actor or threat agent is, whether it is a nation state, organized crime, insider, or some organization to which we can ascribe blame for what occurred and for the damage inflicted. Those less familiar with cyberattacks may often ask, "Why did they hack me?"

These questions are rarely helpful, providing only psychological comfort, like a blanket for an anxious child, and quite often distract us from asking the one question that can really make a difference: "HOW did this happen?"

The current focus on the "who" and the "why" does the industry and our society very little service. We need to rethink and refocus the security risk equation to examine how attacks occur, so we can prevent them in the future.

Let's start by looking at the popular "risk equation" commonly used when assessing the possibility of a breach or cyberattack:

Risk = Threat x Vulnerability x Asset Value or Consequence/Impact

As someone who has been responsible for managing information risk and security in the enterprise for 18-plus years, I have thought through this equation countless times strategically, as well as tactically, during an incident. The conclusion I have arrived at over and over again is that I have little control or influence over threat actors and threat agents – the "threat" part of the

above equation. The primary variable I do have control over is how vulnerable I am – meaning the strength of my present as well as my future control.

From a consequence and impact perspective, there are only three primary consequences we need to focus on: confidentiality, integrity, and availability. Each of these have different potential impacts to an individual, to an organization, or, more broadly, to society, depending on the technology or data attacked. When we examine "how" attacks are accomplished, we see three core targets for attacks:

- Attacks on identity credentials
- Attacks focused on the execution of malware
- Attacks that create a Denial of Service

We must always analyze and report on HOW an intrusion or attack was successful, so we can give attribution to either the control(s) that failed or the lack of control(s) and to those responsible for maintaining proper control.

A great example of this sort of investigation and analysis is the House Committee on Oversight and Government Reform report on the Office of Personnel Management breach, which occurred in September of 2016, and in the subsequent report published in January 2017 by the Office of the Director of National Intelligence on Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution." There are a few important items to note from the upfront background section:

1) "Intelligence Community judgments often include two important elements: Judgments of how likely it is that something has happened or will happen (using terms such as 'likely' or 'unlikely') and confidence levels in those judgments (low, moderate, and high) that refer to the evidentiary basis, logic and reasoning, and precedents that underpin the judgments."

2) The nature of cyberspace makes the attribution of cyber operations difficult but not impossible. Every kind of cyber operation — malicious or not — leaves a trail. U.S. Intelligence Community analysts use this information, their constantly growing knowledge base of previous events and known malicious actors, and their understanding of how these malicious actors work and the tools that they use to attempt to trace these operations back to their sources.

The government — which has badges, guns, jails, and laws to enforce — should continue to focus law enforcement and other government agencies on attribution related to the source(s) of attacks, so they can take action to deter (via conviction and jail time) the threat actors who wish to do harm. They can also post an incident if enough evidence exists and attempt to detain and prosecute those responsible. This alone is a completely insufficient forum of attribution, however, and, per the report itself, has a degree of judgment.

Learning from the History of Attribution

One thing that can be done with complete certainty is to look closely at HOW the threat actors were successful and hold those people and organizations accountable. We can also look back in history and learn how every other reported intrusion occurred in the past decade, including the now-infamous attacks on Sony, Home Depot, the Office of Personnel Management, Yahoo, Target, Anthem, and JPMorgan Chase. This attribution is irrefutable, and the only questions we now have left to answer are why the same story has presented itself over and over again and why we (as an industry) are failing to pay attention to it.

All of these intrusions have been successful, because of one or both of the following:

1) Control(s) that failed, and/or

2) Incomplete or lack of control(s)

We can attribute the source of these items very simply and with certainty by answering two basic questions:

1) Who is accountable for the control environment?

2) Who created the control(s) that failed?

So, whom should we really hold accountable for the success of all these intrusions? The none- too-flattering answer is that while the breached organizations or the creator of the technology that was vulnerable may shoulder some of the blame, we can attribute the success of these attacks in many cases to the cybersecurity industry itself.

Here is the simple reason: The security industry sells controls that fail and do so repeatedly. And here's the rub. These products and services don't just fail in extreme conditions or because of highly unusual or sophisticated attacks. Every one of the organizations that suffered a breach was relying on the capabilities of a security provider that failed to prevent the attack.

Why are these vectors so easy? The simple reason is that in many cases, the security solutions deployed don't work with high enough success rates to make an attack difficult or even challenging.

Disengaging from the Blame Game

In order to move forward and refocus our industry's energies on making attacks more difficult for malicious actors, we need to break free from our own obsessive infatuation with attribution. By investing all of our resources into finding out "whodunit," we get to play the victim card to minimize our own responsibilities and limit our liabilities. None of that helps the organizations that have been breached or the customers and clients who trusted those companies with their private information.

Instead, we need to focus on WHY those intrusions were successful, so we can give attribution to the real source of the intrusion – the controls that failed or lack of control.

This form of attribution will bring real accountability and recalibrate our collective sights to take aim at the one variable in the risk equation that we have real influence over – our strength of control. Then, and only then, can we start to make a difference and put a bend in the curve of risk we have been witnessing, versus continuing to let it grow unchecked.

Control Frameworks that Add Value

I have said for years that the core of business-driven security and the mission of the information risk and security team is "protect to enable." When you are protecting to enable people, data, and businesses, you are proactively engaged upfront and aligned with the business on the evaluation of how to achieve the business objective while best optimizing your controls.

I achieve that through my "9 Box of Controls" approach that was published in September of 2016 in the second edition of my book, "Managing Risk and Information Security: Protect to Enable." My perspective is rooted in my experiences as a business leader and in my many years in finance, including my role as a profit and loss manager for a billion-dollar business unit in the late '90s. It is a control philosophy that I have carried forward in my roles in security, but one that I believe is lacking in the industry.

An important aspect of this perspective is the concept of control friction. The 9 Box of Controls is a simple framework that takes the issue of control friction into account when assessing the value as well as the impact of any control, including information security.

I believe that the 9 Box of Controls includes some actionable perspective that may be valuable to many organizations facing these universal risk challenges. My conversations with peers at other companies have validated this view. Many of them are now using the 9 Box to drive not only tactical but also strategic discussions in their organizations around where they are spending their resources today and where they should be headed long-term.

Types of Security Controls

There are three primary types of security controls:

• **Prevention** occurs when an action or control prevents a vulnerability upfront in the design and development, or stops an infection or cyberattack in its tracks before it affects users or the environment.

• **Detection** means identifying the presence of a vulnerability or detecting something malicious that has already entered the environment.

• **Response** is areaction to the discovery of an issue that has already occured once harm has started and attempting to stop the harm that is already impacting the user or the organization.

From a risk perspective, prevention focuses on minimizing vulnerability and the potential for harm, while detection and response focus on minimizing damage. When you are focused on minimizing damage, the main variables to turn the reactive risk dials are a) time to detect and b) time to contain.

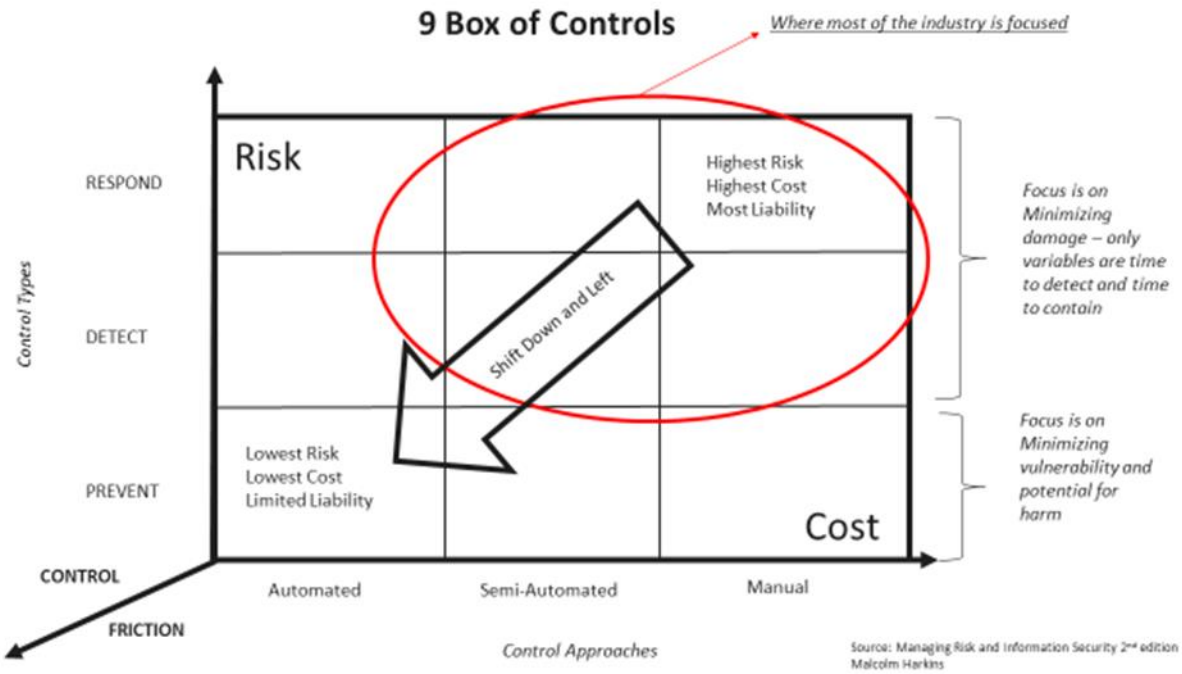
There are also three primary approaches one can take to implement a control:

• **Automated control** occurs entirely through machines.

• **Semi-automated control** involves some level of human intervention.

• **Manual controls** are managed entirely by hand.

The combinations of these control types and automation levels comprise the cells of the 9 Box, as shown in the figure below. Risk increases as we move from prevention to detection to response. Cost increases as we move from automated to semi-automated to manual controls.



Eisenhower warned that we must "not fail to comprehend the grave implications of the path we are on as a nation… We must avoid the impulse to live only for today, plundering … the precious resources of tomorrow." He warned that we cannot "mortgage the material aspects of our grandchildren;" otherwise, we risk becoming "the insolvent phantom of tomorrow."

Edward Everett Hale once said, "I am only one. But I am still one. I cannot do everything, but can still do something, and because I cannot do everything, I will not refuse to do the something I can do."

The RSA conference theme this year was better. For us to get better, CISOs, CSOs, and CPOs need to take control of the industry, rather than be controlled by an industry that by and large has failed us and the organizations we serve. We need to take control of the public policy discussions and implement change to nullify the influence of the cyber industrial complex that has arisen over the past few decades.

As individuals and as a community, we need to force attribution to the control(s) that failed so we can learn from our mistakes. We need to champion transparency to see which approaches and technologies work and which controls create a false sense of security while allowing the risk and spending cycle to continue. If we do this correctly, we can create an incentive for the industry that will accelerate the deployment of controls that reduce cyber risk and reduce the long-term costs to our organizations. This will right the imbalance we have today with the vendors controlling our destiny and reduce the frustration that we all feel with the lack of real progress we have made.

Striving for anything less would be unworthy.