Ransomware:
Why Money is Fueling the Cyber Pandemic

SEPTEMBER 2021

ROB CHENG

Table of Contents

Executive Summary

The cybersecurity industry is broken and unable to deliver in a timely and cost efficient manner the products and services required to counter the growing ransomware threat. "Ransomware: Why Money is Fueling the Cyber Pandemic" analyzes the financial motivations of the cybersecurity ecosystem, including the ransomware makers, the ransomware industry, the media, the security and IT advisors, the cybersecurity workforce and the government. Outside of the ransomware makers themselves, too many factions are profiting disproportionately relative to the value added to the market place. The industry itself has abandoned prevention in favor of reaction, since this strategy maximizes revenue regardless of effectiveness. This white paper concludes that a balanced approach between reaction and prevention will create superior security at a lower cost, and address the ransomware menace head on.

The cybersecurity industry has abandoned prevention in favor of reaction. This strategy maximizes revenue regardless of effectiveness.

Introduction

After 25 years at the FBI, Scott Augenbaum retired to become an author and speaker on the lack of prevention in cybersecurity.

I met Scott Augenbaum, in Myrtle Beach in June 2021 at the Techno Security and Digital Forensics Conference. Scott, a 25 year cyber FBI veteran and the key note speaker, wondered why each year increased money and attention are devoted towards cybersecurity and yet each year ransomware accelerates in the wrong direction. Ransomware is now daily news and its victims are large technically sophisticated organizations, and critical elements of cybersecurity industry. What is happening?

This white paper analyzes the macroeconomics of the cybersecurity economy, and tries to answer Scott's question. It is the hope that this analysis will pinpoint areas of concern, moving constituents towards positive action to correct ransomware's trajectory.

The Ransomware Industry

In September 2013, ransomware infected a woman's Windows computer and encrypted her personal files including photographs, videos, Excel and Word documents. Her files were inaccessible until a ransom was paid in crypto currency. The ransomware was delivered in an email attachment that she mistakenly clicked. The ransomware skated by the computer's antivirus and began its dirty work of sequestering her files. After completion, the computer was unusable and an ominous ransom demand blipped on her screen with a timer. She had two days to pay a few hundred dollars in Bitcoin.

The ransomware industry has blossomed into a high growth, high margin business extracting millions of dollars daily from its victims under the cloak of anonymity that have left law enforcement helpless.

From these humble beginnings, the ransomware industry has blossomed into a high growth, high margin business extracting millions of dollars daily under the cloak of anonymity that have left law enforcement helpless. Over the last eight years, the number of ransomware incarcerations can be measured on one hand. What is known, is that the perpetrators are outside of the country, and although media speculates the ransomware is made in Russia, there is no hard attribution that would hold up in court. The enemy for all intents and purposes is anonymous and outside of American law enforcement.

In March 2021, CNA Financial, the nation's 7th largest commercial insurer paid a $40MM ransom to recover operations, and hopefully not have their client's information dumped on the web. Although the perpetrators are unknown, one can imagine. Think of a small team of five people living in a foreign and financially repressed region of the world. The team works industriously for a few months, learning everything about ransomware. How to build the ransomware, finding security holes, deploying ransomware, demanding a ransom, receiving payment and helping victims retrieve their files.

There is little barrier to entry to making ransomware. Rather than focusing on perpetrators, more attention should focus on the security holes through which the ransomware enters.

The Ransomware Industry

Ransomware is not a complicated technology or business and none of these assignments were particularly difficult for these smart, financially motivated young people. Then they hit the mother lode, CNA Financial. This small ransomware team are millionaires. Post pandemic, the dollar is unusually strong, so in their local countries, our little imaginary team are among their country's financial elites.

The team that hit CNA Financial has created a simple business model on how to become a millionaire almost overnight and get away with it.

The media paints the ransomware industry as being from a particular region of the world. There is no evidence that this is true, and even if it were, it need not be that way. The only tools to be part of the ransomware gold rush are an internet connection, a computer, a VPN, and other obfuscation tools. They could be in any country in the world, and most likely are, and if not, most likely will be.

Our little team that hit CNA Financial has created a simple business model on how to become a millionaire almost overnight and get away with it. This process is being replicated throughout the world. These people are not villains, they are opportunists that have created a business monetizing the world's security holes. The US is frequently targeted because America has more computers per capita than any other nation. Willie Sutton, when asked why he robbed banks, famously responded, "That's where the money is." America is where the money is.

CNA Financial paid a whopping $40M ransom validating the ransomware business model.

The Cybersecurity Industry

One would think that if the ransomware opportunists are monetizing security holes, then the logical response would be to close the security holes. Sadly, that is not the vision. Rather than closing security holes, the mission is to allow the ransomware to enter the network and monitor in real time its behavior for suspicious activity. Once the suspicious activity is confirmed, the ransomware can be terminated and the damage is minimized. The name of the strategy is "detect and respond", and is the advent of the 24/7/365 SOC (Security Operations Center). There are numerous flaws to this strategy.

> **The mission is to allow the ransomware to enter the network and monitor in real time its behavior for suspicious activity.**

- **Excludes Prevention.** Unless the ransomware can be 100% confirmed malicious, it enters the network for surveillance. The advent of the EDR (Endpoint Detect and Respond) and XDR (Extended Detect and Respond) strategies preclude preventative solutions because prevention is supposedly futile.
- **Viruses Move Faster Than Humans.** The internet accelerates the rate at which information good or bad moves from point to point. A virus in a network is moving at this increased velocity that is at a minimum 1000x faster than humans can process.
- **Human Error.** EDR introduces human error into a zero tolerance environment. It is not hard to imagine that a sleepy technician misses a threat because he was just served divorce papers.
- **Expensive.** The hardware and software to create a SOC and the manpower for constant surveillance is spendy and out of reach of many segments of the marketplace including small business, K-12, cities, counties, police departments, etc. These unserved segments of the markets were some of the first to pay ransoms and gave the ransomware the oxygen to evolve into its current form.

As ransomware escalates, the country's response has been to build more Security Operations Centers (SOC), which has been a boon for the cybersecurity industry.

The Cybersecurity Industry

Despite these flaws and criticisms, the SOC excels at one thing exceedingly well, driving revenue for the cybersecurity industry. The SOC is the golden ticket of Cyber's Got Talent. During the cyber gold rush, normal business economics no longer apply. Investors in cybersecurity companies don't analyze profits and cash flows and focus on one metric, revenue. A manic sprint to the bottom has ensued to discover which cybersecurity company can achieve the highest revenue growth regardless of the size of the losses. Now rather than a multiple of earnings, cyber companies are valued on a multiple of revenue and the multiples are stunning. Some of these companies trade at 60 to 100 times annual revenue. It is doubtful that most of these companies will exist 60 to 100 years from now, but here we are.

The cybersecurity industry can be characterized as high revenue and high losses funded by public and private equity regardless of the effectiveness of these solutions.

Private and public equity are financing the losses of select cybersecurity companies as long as they drive revenue. It gets better. Because the SOC is flawed for the reasons stated above, and ignores more budget conscious segments of the market, the cyber posture of the nation deteriorates. The reaction from governments and enterprise is to provide additional cybersecurity funding. As those budgets are allocated, the first in line are the revenue hungry, profits be damned, cybersecurity industry.

An interesting example is the $2B cybersecurity bill that recently passed the House and the Senate. The cyber reaction companies that make and man SOCs will receive the lion's share of this allocation, elating their stockholders as the nation reacts more and prevents less of these cyber threats. This unhealthy relationship between ineffective cybersecurity strategies, revenue hungry companies with losses funded by the equity markets, and increased annual cyber allocations due to the deteriorating conditions is a spiral that is driving the country mindlessly full throttle to the brink.

Opacity

The enormous economic losses in the cybersecurity industry is a distortion in the market place rendering buyers unable to find the best solutions. Ransomware entrepreneurs operate in the dark due to anonymity of cryptocurrency and so does the cybersecurity industry due to reasons unknown.

The perfect example of the cyber opacity problem is the Colonial Pipeline ransomware shutdown. Colonial Pipeline was worldwide news and the shutdown lasted a week inconveniencing millions of people in the southeast of the country. Ransomware awareness reached a secondary high and despite dozens of private and public investigations, Congressional inquiries, and every news outlet in the world yammering for an angle on the story, certain details never came out.

Despite the national media coverage of Colonial Pipeline, critical information was never uncovered such as what antivirus failed that led to the infection.

The public needs to know the details of Colonial's cyber attack to identify the security holes in their stack that permitted this highly public infection. For every ransomware infection, there is a failed antivirus that allowed the ransomware on the network. What antivirus was Colonial buying? Did Colonial have a SOC? One would think so, but these details were never divulged. Did someone fall asleep at their computer?

Without this critical information, buyers are unable to make informed decisions. We know that an antivirus failed but the public never learns which one. Since the Colonial infection was so high profile, that antivirus should be getting pounded. Current customers of that antivirus should be looking for an alternative, and their stock price should be tanking. The market place cannot weed out flawed strategies and products due to opacity.

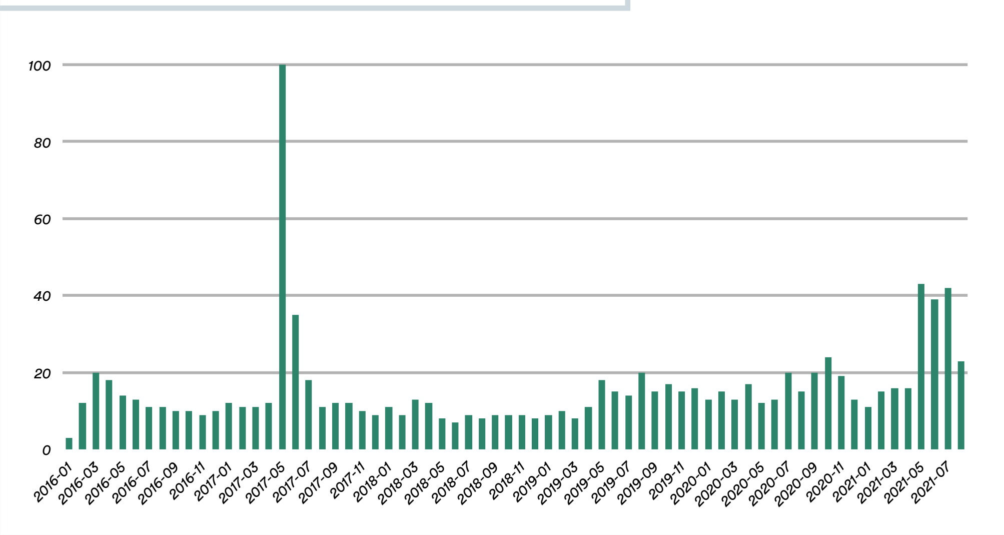
An interesting contrast is the television market. In the last decade, the industry has had numerous high profile failures including curved televisions and 3D televisions, in a blind search to get people to dump their 8 year old HD TV for a new shiny new one. The market place responded, and the industry reacted and dropped these failed initiatives. The market place is unable to give the proper feedback to the cyber industry due to opacity. The ransomware beneficiaries are the cybersecurity industry and the groups that make the ransomware. The public suffers.

The Media

Back in the day, large and highly profitable computing magazines dominated newsstands worldwide. Readers would anxiously read the latest copies of PC World, PC Magazine, and Byte for the latest developments and products in the personal computer revolution. Advertisers like Gateway and Dell ran 12 page extra thick inserts attracting a new sophisticated buyer of high technologies. It was an economic love story.

Journalists, many household names, made it their life's work to keep us informed on the latest developments and sometimes their lofty opinions on said technology and the personalities of the rock and roll PC revolution. But then, the internet happened and slowly and gradually eroded the revenue and dominance of these once esteemed brands. As their outlook declined, layoffs and restructures were common and many of our favorite journalists either retired or were let go. PC journalism was replaced by freelancer writers that viewed each article as a homework assignment rather than a profession.

Ransomware Awareness



Ransomware awareness has reached a secondary high, due to the high profile infections at Colonial Pipeline and Kaseya. Source: Google Trends

The Media

Things looked rather bleak for IDG and Ziff Davis, the parent companies of the storied publications of the 90s. But, then a savior, ransomware, rose from the ashes and swooped down to their limping carcasses and breathed new life and energy to their flailing web site traffic.

> **Security should be boring. Only when systems fail is it newsworthy.**

After each new and horrific cybersecurity mishap, readers flock to learn, observe, and gossip about the latest cyber train wreck. Every year, the cyber press document every detail of the country's digital demise as if it is a fait accompli. As the nation's cybersecurity further declines, main stream media jumps to center stage. Recent breaches are covered nationally on Fox News, CNN, CNBC, Fox Business, ABC, NBC, and CBS. 60 Minutes has done numerous segments. Even Jon Oliver, a comedian, did a recent ransomware segment. It is stunning that with all this media attention, not one has covered the security holes through which the ransomware is entering. Instead, the focus is on the damage to society, the legal harm to the victim, and the highly speculative country of origin of the perpetrators. In terms of cybersecurity, the media has taken a front row seat of the nation's slow march toward cyber Armageddon. They've built a whole business model around it.

Ransomware was a needed lifeline to the tech media that's revenues and profits had been declining for over a decade.

Here's the rub. Security should be boring. Only when systems fail is it newsworthy. When systems fail, work should be done to rectify the failures and time and time again, the issues remain unaddressed. For every public infection, there should be valuable lessons regarding which security holes the virus entered, and how those holes can be closed to avoid further infections.

Technology Advisory Firms

Accenture is perhaps the world's largest, consulting and professional services company, with revenues topping $44B and over 569,000 employees. Last year, Fortune Magazine awarded Accenture the world's most admired Information Technology Services company. A significant portion of Accenture's practice is cybersecurity consulting, advice and professional services. Accenture was infected with ransomware in August 2021, with a reported 2500 computers infected and 6 terabytes stolen.

Tech giant, Accenture, falls to ransomware forcing the public to wonder of value Accenture's cybersecurity advice.

Accenture has an almost unlimited budget to spend on cybersecurity, and certainly can choose the best of breed solutions that many of their advisors recommend. For sure, Accenture has a Security Operations Center, and somehow, someway one of the giants of cybersecurity have fallen.

A good friend from a different Technology Advisory Firm confided, "We follow the industry and lead our customers." In every way, my friend's comment is true. The cybersecurity industry is going in a dangerous direction, and not just Accenture but every other technology advisory firm will echo the voice of the industry. These firm's analysts will make distinctions and pick favorites between different companies in cybersecurity but if the direction of the entire industry is incorrect, that will be echoed to their customers.

Accenture and the technology advisory industry benefit from the same inverse effect as the rest of the cybersecurity industry. When their advice is incorrect, the ransomware accelerates, and their revenue grows as the confused public looks for answers. Accenture, as well as Solar Winds and Kaseya, are among the cyber elites gasping for air.

Cybersecurity Insurance

When the pain of ransomware and the panic in the public became visceral, the insurance industry pounced to monetize the fear.   Cybersecurity insurance, launched circa 2016, was deemed a godsend to the impending escalation of ransomware and monetization of the nation's security holes. After filling out a rather simple form, any institution, big or small, public or private, could be protected from the most sophisticated cyberthreats. Some speculated that cybersecurity insurance would become mandatory, similar to car insurance in most states. Five years later, the wheels are falling off the cybersecurity insurance bus.

Cybersecurity insurance is suffering due their inability to assess the rising risks related to ransomware.

Since 2013, the advent of modern ransomware, the FBI's one consistent message has been "Don't pay the ransoms." With a cybersecurity insurance policy in hand, the holder could demand that the bank pay the ransom post infection. In 2019, Lake City, Florida, a small town of 12,000, paid a whopping $460,000 in untraceable cryptocurrency for the retrieval of its files and restoration of operations.   A town of that size would never have been able to pay a ransom of that magnitude, but now they could. Prior to cybersecurity insurance, ransoms were typically between $10,000 to $50,000. For example, in 2018, the city of Atlanta went down, and refused to pay the $51,000 ransom.

Once the cybersecurity insurance industry opened the money spigot, dollars flowed like a river out of the country. The reason the FBI advises to avoid payment to minimize the chance of future ransomware. Cybersecurity insurances contributed to 1) rise of ransom price levels, and 2) the increased probability of infection.   None of this was factored into their actuarial models.

Today, cyber premiums have tripled in the last year, and the banks know that the policies they've written are bad bets, and are desperately trying to wiggle out of them.   The current models employed by the banks are insufficient to measure the cyber risk in the country as a whole or an individual institution. Perhaps new cyber risk models can be established but the situation is evolving and is no easy task.

Ransomware is commonly referred to as a computer virus, but a more apt analogy is a cancer. The cancer metastasizes each time a ransom payment is received. Money is ransomware's life blood. The cybersecurity insurance industry unwittingly moved the ransomware cancer from Stage 2 to Stage 3.

The Work Force

The focus on cyber reaction instead of cyber prevention has driven a shortage of cyberworkers. Each time that Congress allocates more funds, the shortage becomes more acute. The result is a focus on quantity of cyberworkers, rather than quality. The average skill and knowledge of cyberworkers has been declining for years. The result is a sense of mediocrity in cybersecurity as the nation searches for answers from a work force focused on a bigger house or a new boat.

Those in cybersecurity feel like they won the lottery and they don't want the party to end.

It has never been a better time to be in cybersecurity industry, the shortage has driven an inflation of salaries and other benefits. Veterans of the Great Cyberbubble are now retired and millionaires and more likely multi-millionaires. As the veterans make their financial exit, they are replaced with inexperienced cyber rookies continuing the drive to cyber mediocrity. Marginal cyber employees thrive in such an environment hopping from one cyber company to another, accomplishing little, other than padding a sketchy resume. Companies desperate to share in Congress's cyber largesse hire almost any applicant with a pulse, and the word "cyber" in their CV.

The worse cybersecurity in America becomes, the more money flies to the problem which has caused a shortage of cyber workers inflating salaries and creation a mediocrity in the work force.

The dichotomy in cybersecurity is between the people inside of the cybersecurity industry, and those on the outside. Those on the outside see an escalating ransomware problem impacting millions daily requiring large changes in the nation's cyber posture. Those on the inside feel like they won the lottery and they don't want the party to end.

Advice

With mediocrity raining down on cybersecurity, good cyber advice is extremely rare. The Colonial Pipeline infection impacted millions of citizens, driving ransomware awareness to new heights, and prompted a flood of advice on how to deal with the ransomware problem. Post Colonial Pipeline, a study analyzed the quality of ransomware advice across dozens of web sites including the tech media, main stream media, and the government. The study found that the #1 recommendation across the myriad of advisors was to backup critical data.

The cybersecurity industry is driving the country to an uncomfortable precipice.

This recommendation could not be more wrong. The FBI advised in late 2019 of a new ransomware, Sodinokibi, that steals critical information before encrypting. If the ransom is unpaid, the information is exposed on the public web, as another inducement to pay the ransom. Before that, the FBI advised that ransomware upon entry on the network, would first disable the backup. Even if the backup survives, and the data was not exfiltrated, restoring from backup can be time consuming, frustrating, and difficult. For example, the city of Atlanta took six months to restore operations after refusing to pay the ransom. The cost to the city of Atlanta was far greater than the ransom, even though they restored from backup.

The Federal government isn't much better. The newly created CISA (Critical Infrastructure Security Agency) pushed backup as the best prescription for ransomware in March 2021. With great anticipation, the Biden administration reinstated a National Cyber Director. Ann Neuberger, speaking on behalf of the National Cyber Director, encourages businesses of all sizes to implement Endpoint Detect and Response (EDR) and multifactor authentication. Although this advice is great for large and rich organizations like the Federal government, it is not appropriate for small businesses, K-12, cities and police departments. Neuberger omitted prevented measures such as application whitelisting, which represents a lost opportunity.

The cybersecurity industry is driving the country to an uncomfortable precipice. An alternate voice to the cybersecurity industry is essential for the country to find its way during these uncertain times. Biden's National Cyber Director is a step in the right direction, but its potential remains largely untapped.

The Government

In January 2009, President-Elect, Barack Obama, met a few weeks before inauguration, with outgoing George W. Bush to discuss transitions. “One thing I wished I had accomplished was shutting down the Iranian nuclear reactors through an NSA initiative called Stuxnet.”, the Texan drawled. Obama, dealing with a financial crisis, but eager to please, unleashed Stuxnet, a little over a year after taking the helm.   The attack was successful shutting down three reactors, setting back Iran’s nuclear ambitions a decade, and bringing Iranian leaders to the negotiation table to discuss nuclear proliferation. Still today, the Stuxnet attack is considered the most sophisticated and successful cyber attack.   No American set foot on Iranian soil.

Early in Obama’s presidency, he authorized a sophisticated cyber attack on Iran shutting down three nuclear reactors, however the NSA tools were hacked and accelerated ransomware.

The Iranian government, licking its wounds, post Stuxnet, constructed a national cyber program that is considered to be one of the most sophisticated in the world. The Iranians joined forces with the cyber programs of other American adversaries such as North Korea, and successfully hacked the NSA. The cybergang stole many of the NSA’s most important technologies including the tools used for the Stuxnet attack. Once hacked, this treasure chest of hacking tools made its way to the Dark Web and ultimately to the nascent ransomware industry.   With the NSA Stuxnet tools as jet fuel, a new ransomware, WannaCry, was unleashed in mid 2017 and remains the most successful ransomware attack. WannaCry infected over 200,000 computers in 150 countries in less than a day, exposing the gross deficiencies in the world’s defensive capabilities to the upcoming ransomware offensive. Shortly after WannaCry, another global ransomware, NotPetya, was deployed on a wobbly public hitting numerous victims including shipping giant, Maersk Line, the Ukrainian nuclear reactor, and many American casualties including the city of Baltimore.

The Government

Stuxnet serves as an example of the pluses and minuses of the American government. The DOD was able to unleash the world's most successful nation state cyber attack, but was unable to protect and safe guard the tools that made Stuxnet so successful. The focus of the DOD still today is developing the tools and the intelligence to attack other nations.

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
UNITED STATES DEPARTMENT OF COMMERCE
100 Bureau Drive

Since 2015, NIST has been the voice of prevention in battling cybersecurity which has driven programs in the federal government, but unfortunately this important message has not been heard outside of the federal government.

Both the WannaCry and NetPetya viruses, ran amok through exploiting vulnerabilities in the world's software base. A vulnerability is an unknown security hole in a commonly used software, such as Microsoft Windows. Once the NSA was hacked, many of these unknown vulnerabilities surfaced much to the detriment of societies throughout the world. Still today, the DOD stockpiles these vulnerabilities frequently paying millions for a high profile vulnerability. Rather than closing security holes, the DOD promotes holding them for future use against potential adversaries.

During this cyber mayhem, the National Institute of Standards and Technology (NIST) published Report 800-167 called Guide to Application Whitelisting in late 2015. NIST is perhaps the world's most influential authority for standards and technology. From the document, "NIST advises organizations to use modern whitelisting programs (prevention), also known as application control programs, to stop cyber threats."

NIST's influence was immediate changing the civilian CDM program (Continuous Diagnostics and Mitigation) to require application whitelisting in compliance with NIST controls. Later in 2019, the CMMC (Cybersecurity Maturity Model Certification) followed suit and requires application whitelisting for levels 4 and 5 certification for all DOD contractors.

The Government

NIST is the voice of prevention in the nation's cyber dialog with the DOD representing the nation's cyber offensive capabilities, and the cybersecurity industry focused on monetizing reaction to an escalating threat. Although NIST has had success impacting the federal government, NIST's message of prevention has been lost in the noise outside of Washington DC. Enterprise, state and local governments, and small businesses, are advised to quickly learn how to react to a ransomware infection after the point of infection with little regard to preventing the ransomware in the first place.

As ransomware and other cyber threats escalated unabated, in 2018, President Trump stood up a new cyber agency called CISA (Critical Infrastructure Security Agency) reporting into the Department of Homeland Security. CISA's charter is to be the primary contact between the government and private sector on cyber issues, share threat intelligence, respond collectively to cyber attacks, and build a more secure and resilient cyber infrastructure. Through personal experience, in practice, CISA has moved to be the focal point on breaking cyber attacks. For example, during the massive Solar Winds infection, CISA worked with Solar Winds installed base inside and outside of the government to move to the latest version of Solar Winds Orion which had not been compromised. Although CISA has a broad charter, most of the efforts are focused on reaction putting CISA in line with the cybersecurity industry.

President Trump launched a civilian cyber agency, Critical Infrastructure Security Agency (CISA) in 2018. CISA focused on public / private partnership and reaction to events and little on prevention.

Last but not least is Congress that strictly reacts to the shocking increasing scary ransomware news. Lately, every week brings a new ransomware crisis and as Rahm Emanuel once gloated, "Never let a serious crisis go to waste." Each year, Congress passes an increasingly generous cybersecurity funds which continue to reward the industry that created the problem in the first place.

Prevention – The Missing Piece

Lost in the entire conversation is cyber prevention. The three pillars of prevention.

1. **Cybersecurity training.** Organizations do allocate for training, but these spends are dwarfed by the budgets for cyber reaction.   There are some areas of cyber that can only be solved through training. For example, spotting a compromised email address can only be accomplished through training. It is concerning that many people are entering the workforce without basic cybersecurity training and awareness. However, training is imperfect, and at times retention rates are poor.
2. **Multifactor Authentication.** Multifactor authentication is effective and has high awareness. MFA is, however, expensive and unreachable for smaller, resource constrained organizations. MFA is tricky to deploy in its entirety. Even larger organizations may not have deployed completely leaving security holes. Most importantly, not all ransomware infections are a result of an authentication breach. Even with perfect adoption, security holes remain.
3. **Application Whitelisting.** The most effective method to eliminate ransomware is application whitelisting which strictly allows known good programs, and any divergence and anomalies are proactively blocked. Application whitelisting has low awareness despite the recommendation by NIST and adoption in the federal government.

Prevention is more than a list of technologies and products. Every breach or infection represents an opportunity through which security holes the compromise occurred. The prevention mindset is to rapidly close security holes after their discovery. This mindset should be present in the media, government, the cybersecurity industry, and the public.

Conclusion

The economics underlying the cybersecurity industry are broken. Each week, cybersecurity continues to wreak havoc on citizens and businesses, and there is insufficient incentive to "fix" cybersecurity. By focusing strictly on reaction, rather than prevention, the cybersecurity industry maximizes revenue at the expense of their customers and society as a whole.

The drum beat of reaction instead of prevention is so loud from the media, the industry and the government that even the prestigious NIST cannot break through the noise and the market is unable to find the most appropriate solutions.

Prevention is practical, economic and normally not newsworthy. Application whitelisting stops the ransomware by design while occasionally blocking a good file. This architecture is designed to complement the security stack of any organization large or small. It's time to get well.

Prevention is practical, economic and normally not newsworthy.

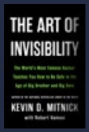
Cybersecurity Reading

This is How They Tell Me the World Ends
Nicole Perlroth

2034
Elliott Ackerman

The Age of Surveillance Capitalism
Shoshana Zuboff

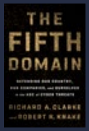
Dark Mirror
Barton Gellman



The Art of Invisibility
Kevin Mitnick

The Dawn of the Code War
John Carlin

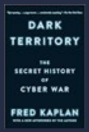
The Hacker and the State
Ben Buchanan



The Fifth Domain
Richard Clarke

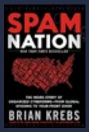
The Shadow Factory
James Bamford

Sandworm
Andy Greenburg



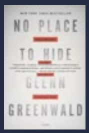
Dark Territory
Fred Kaplan

Permanent Record
Edward Snowden



Spam Nation
Brian Krebs

World Without Secrets
Richard Hunter



No Place to Hide
Glenn Greenwald

About the Author

Rob Cheng is the CEO and founder of PC Matic. Rob is best known as the company's spokesperson on their numerous direct response television advertisements on Fox News, CNN, MSNBC, and others.

Cheng has over 40 years experience in the sales, marketing and support in the computer industry. Prior to founding PC Matic in 1999, Rob was the SVP of Gateway Computers driving sales, marketing, and support worldwide.
Rob began his career at Texas Instruments responsible for sales, marketing and support in Latin America.

Rob holds a BS in Engineering from Cornell University and an MBA in Finance from the University of Texas.

Rob Cheng
PC Matic CEO and Founder

Note from Rob

Recently, various people in cybersecurity begin their writings with “Let’s assume ransomware is here to stay.” There is a way to stop ransomware and I wrote the white paper to demonstrate a very viable alternative. Prevention is more than a set of products, or recommendations, but a mind set required to override the reactive mindset pushed by the cybersecurity industry.

Thank you for reading my white paper, and if you want to see a new direction in cybersecurity, please send the white paper to your most important and influential contacts.