

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

WHITEPAPER

THE FUTURE OF CYBERSECURITY



NIGHTDRAGON
SECURITY



With Thought Leader and Visionary, Dr. David G. DeWalt

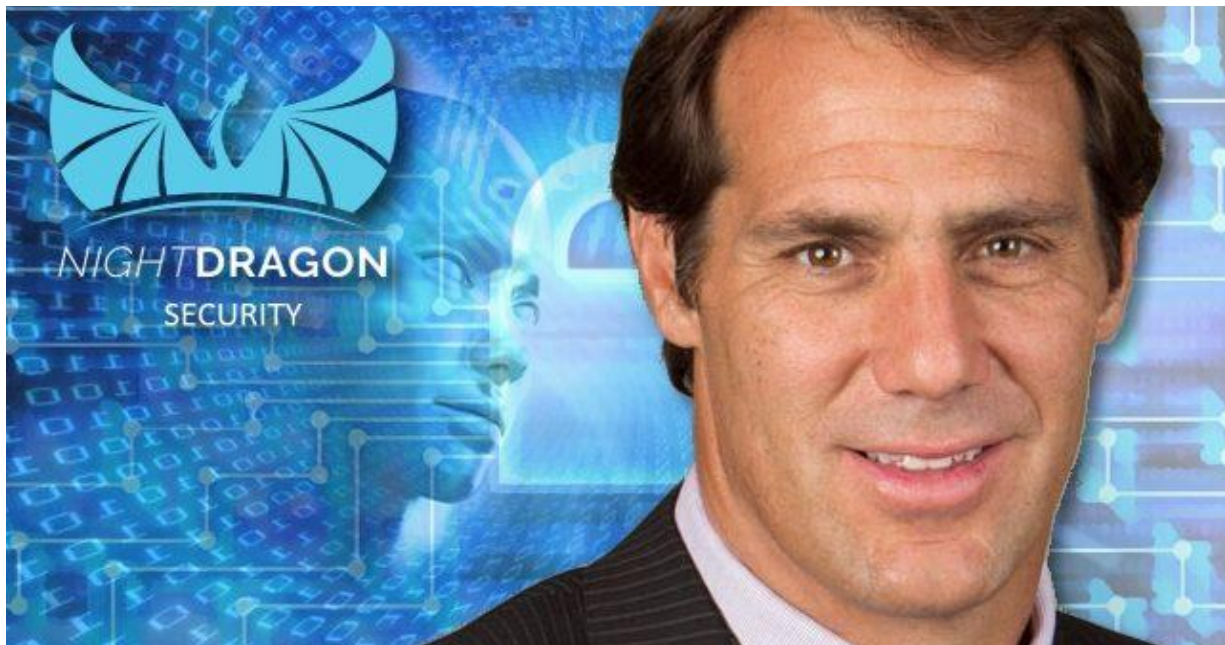
Contents

The Future of Cybersecurity	3
UNDERSTANDING THE FUTURE OF CYBERSECURITY	3
LOOKING BACK	4
FORGET LAWYERS AND BREACH NOTIFICATION ACTS: DO THE RIGHT THING ..	9
TURNING A HUGE NEGATIVE INTO AN EVEN BIGGER POSITIVE.....	10
SUMMING UP THE PAST, PREDICTING OUR CYBER DEFENSE FUTURE	10
WE'VE ENTERED THE PERFECT STORM IN CYBER DEFENSE	11
What's driving the perfect Cyber storm?	13
A PERFECT STORM BRINGS A PERFECT OPPORTUNITY FOR INVESTING... ..	13
INVEST IN NEXT GENERATION DEFENSES	14
DRONES & DOMES	15
INDUSTRIAL & IoT	16
SOCIAL & SATELLITE	18
CLOUD & CRYPTO	20
MOVING THE CYBER DEFENSE MARKETPLACE FORWARD AT LIGHT-SPEED... ..	22
THIS WHITEPAPER IS ONLY THE TIP OF THE ICEBERG	22
BONUS TAKEAWAY TO SHARE WITH YOU	24

The Future of Cybersecurity

With Thought Leader and Visionary, Dr. David G. DeWalt

by Gary S. Miliefsky, Publisher, Cyber Defense Magazine



UNDERSTANDING THE FUTURE OF CYBERSECURITY

When you finish reading this article, and I recommend you read it two or three times, you will have a keen understanding of where the future of Cyber Defense is going from one of the most brilliant and successful minds in the industry.

I had the opportunity and honor to catch up with one of the most talented and innovative movers and shakers in our industry, yet someone who lives by what he preaches – the 3 H's – Honesty, Humility and Hard-work – none other than David G. DeWalt, the founder of NightDragon Security who is also a partner at Allegis Cyber and Momentum Cyber among about 14 or 15 other ventures and activities, to name a few – he's also Vice Chairman of Delta Air Lines as the Safety/Security board member so he is boots on the ground in critical infrastructure as well. He's also serving on the National Security Telecommunications Advisory Council for the US Government. It was refreshing to hear David speak at the **Cyber Investing Summit in New York City** and then to follow it up with a one-hour deep dive into his strategies and platforms.

I assure you, this article, learning who David DeWalt is, where he is investing and what he's predicting could be the most important piece of Cyber Defense Intel for 2018 and beyond.



Pictured Above, NightDragon Security is David's Cybersecurity Platform. More on this later in the article...

LOOKING BACK

A brief backgrounder on Dr. David G. DeWalt

Let's go back in time and then work our way into not only the present, but the future – David takes us on an incredible journey but before we strap ourselves in for what will be an incredible and wild ride into the future of cyber defense, we need to understand where it all started for David.

He has more than 30 years of high tech experience. I think his three H's come from a great upbringing by what most would consider a blue-collar family in the Steel and Coal mining belt of Pennsylvania. He grew up in Reading, PA and with the love and inspiration from great parents, he began his journey, always reflecting on where he came from, keeping his humility intact even after some of the most amazing accomplishments in our space.

Our discussion reminded me of a common thread with great people like **Robert Herjavec** – always questioning and learning and maintaining a high degree of honesty and humility while always willing to put in the long and hard hours. It seems that we can

learn from these successful pioneers in our industry – great minds and successful individuals do think alike and usually start from humble beginnings.



Pictured above, hard work, dedication and perseverance he receives his PhD

A few years ago, David had the honor of giving the commencement speech at the University of Delaware and from this speech we're able to learn a lot about David DeWalt. It was May 30, 2015—David G. DeWalt, chief executive officer and chairman of the board of FireEye Inc., delivered the Commencement address at the University of Delaware, where he graduated in 1986. [At the ceremony, he also was awarded an honorary doctor of science degree.](#)

One of David's favorite quotes comes from the song by OneRepublic, *I Lived...* "Hope when your moment comes, you say, 'I lived.' With every broken bone, as the lyric goes, "I swear I lived." David, as his Dad would say, 'wrestled' his way through college – he was in the 177-pound weight class. Wrestling is a very demanding sport — lots of sacrifices, very few rewards.

Now, Dr. David G. DeWalt is 6 feet and 4 inches and back then he weighed about 220 pounds, so the 177-pound weight was very difficult for him to maintain. Oftentimes he had to go without food and water for days trying to make this number. Oftentimes, he would have to work out countless hours with layers of sweat suits on to make this number.

He suffered enormous hardships during his wrestling career, including breaking his collarbone, dislocating his shoulder, two knee surgeries, cauliflower ear and even losing his front teeth participating in this sport. Swap this coach for David's wrestling coach and swap the sport from Football to Wrestling and you'll understand Dr. David G. DeWalt's [philosophy on life, business, blood, sweat and tears](#). "You are the most influential player on this team, if you walk around defeated, so will they...Don't tell me you can't give me more than I was seeing. God's gifted you with the ability of leadership, don't waste it."

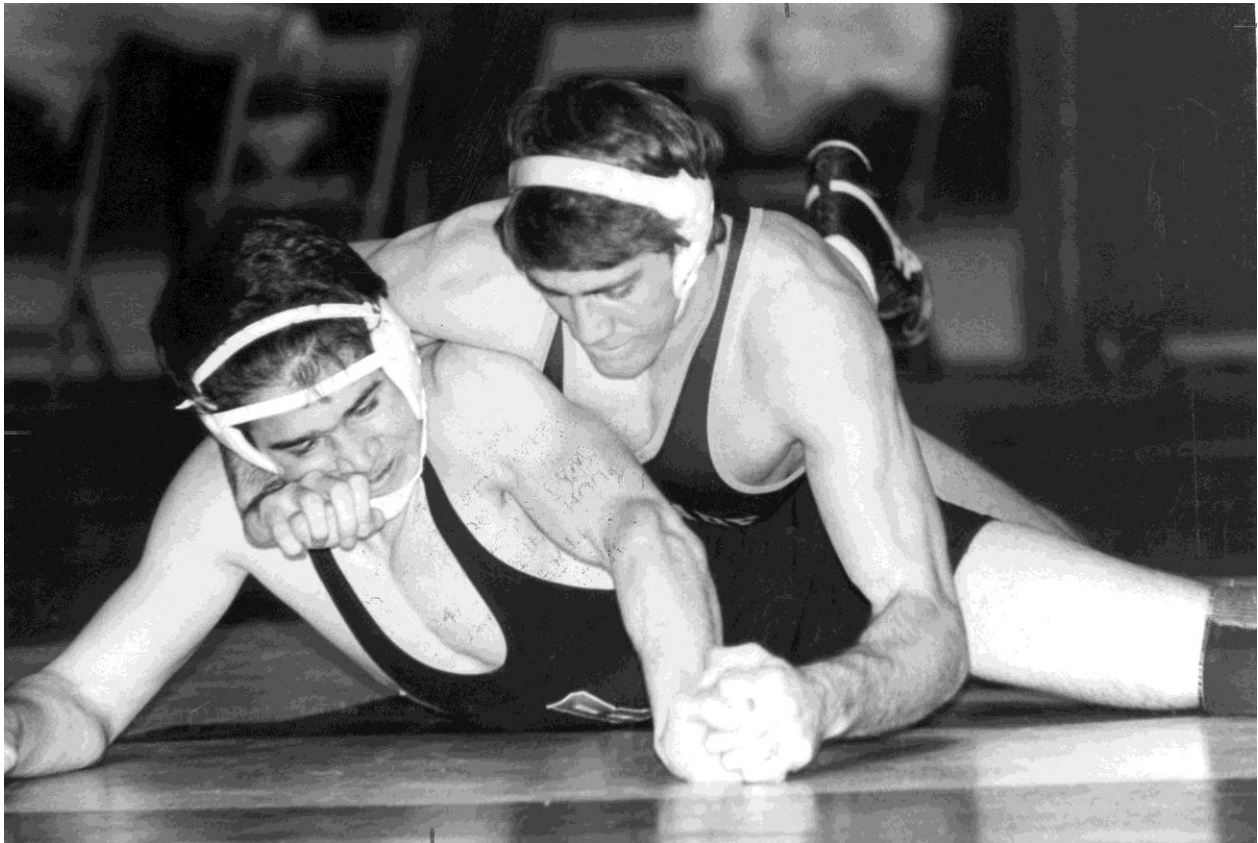


Photo Source Bluehens.com – One of the finest wrestlers in Blue Hens history, DeWalt was inducted into the University of Delaware Athletics Hall of Fame in 2003

Through it all, he wrestled 110 matches for the University and won 101 of them – with his parents watching every single match. His parents taught him much about patience and perseverance. They drove 20 hours up to Boston and back to Reading PA just to watch him wrestle against Yale and Boston University. He finished his matches in under a minute. Think about it. Less than a minute, winning both matches but 20 hours of driving to watch him. We could all learn a lot from David's parents. This kind of dedication breeds winners and leaders – the more involved in our children's lives, the less we will have to worry about their future – it's an incredible investment – and yes, it takes a great deal of

self-less-ness but as David learned and shares, this is one of his strong beliefs that he intends to pass on to his children.

He finally stood on the podium that day, in front of 16,000 fans at the University of Iowa Hawkeye stadium — as an NCAA Division I All-American, the first ever from the University of Delaware. The blood, sweat, and tears of 16 years of hard work, perseverance, dedication and determination had paid off.

“You have to take a leap if you want to attain your goals. I had achieved one of my goals. And there, up in the third deck, were my parents. Always there, always supportive. To this day, I will fly from wherever I am in the world to see my kids perform. Whatever it is they do, I will be there like my parents were for me. Love, live and remember humility is everything. Remember where you are from and don’t ever forget what your loved ones have done for you. Be present. Always alive. Always live on the edge of tears. Always push yourself to be better,” he said at this very memorable and timeless commencement speech.

Words to live by.

Moving forward, David DeWalt graduated with a computer science degree in hand, he decided to pack up his bags and move to California to continue to reach his goals and strive for his dreams. His father thought he was crazy and would be back to Reading, PA, soon. His dad said “California, what’s out there?” And David responded, “Opportunity, Dad. You wait and see.”



So, he drove his **little blue Pontiac T-1000** car across the country and decided to stay in the heartland of opportunity – Silicon Valley, California! There he was, no job, no friends, 3,000 miles away, when he began his high-tech career.

So, now you can understand his three H’s – Honesty, Humility and Hard-work.

Starting with nothing, risking everything, he made it to Silicon Valley. He interviewed with a now famous man named Tom Siebel at a company called Oracle. Tom ran a division called DMD that did direct marketing and tele-sales. During his interview, Tom told him

how people with engineering degrees usually fail at sales and don't have what it takes. David said, "give me a chance – hire me and I'll prove I can do it". His dad wasn't so pleased – an engineering degree apparently going to waste. What David did, was prove them both wrong – like the "Larry Bird" era of the Boston Celtics, David was the first in and the last out every day. This is what made Larry Bird so great and so famous. He also had the humility to admit he wasn't the greatest or the best, but he was the hardest working at his job. And because of this passion and drive, he became one of the very best at his job. He made his numbers, he became the top sales earner at Oracle. He was promoted 5 times during his career there and learning valuable life lessons along the way.

"You have to take a leap if you want to attain your goals. Remember where you are from and don't ever forget what your loved ones have done for you. Always live on the edge of tears. Always push yourself to be better."

Dr. David G. DeWalt, www.NightDragon.com

Pictured Above, Quotable from Dr. David G. DeWalt

Fast forward – greatest failures, leading to greatest successes. The day was April 21, 2010. David DeWalt was proudly the CEO of computer security company McAfee. On this day, he received an urgent call at 6 a.m. to quickly come into the office. As he gathered together with his management team to hear the bad news, he had learned that they

accidentally sent out a faulty release — number 5958 — of their anti-virus software, that McAfee had wiped out every computer in 1,672 companies in 16 minutes.

“When I say wiped out, this is an understatement. Entire companies were unable to boot any computers. Entire companies were unable to operate their businesses. In an effort to stop a particularly nasty threat from a government nation state source, we had accidentally shutdown all the computers that updated with our software that morning,” he said.

Fortunately for McAfee, one of their engineers realized the mistake and rolled the release back, and in the process kept tens of thousands of more companies from updating the faulty release as well.

FORGET LAWYERS AND BREACH NOTIFICATION ACTS: DO THE RIGHT THING

It's so important to always tell the truth. Take ownership. Be honest.

Subsequently, he made an incredibly important decision that day. As the news leaked out and McAfee and his face being prominently displayed on nearly every TV in the world, as their stock dropped 40 percent, decisions needed to be made. Not a good day if you are a CEO. But, in adversity there are always true tests of leadership, and this day was one of those for David DeWalt.

As swarms of media gathered in his lobby for a statement, he made an important [corporate video](#). Against the advice of every lawyer that could reach him, he decided to quickly publicly air what had happened. He took full responsibility for the actions of his company and apologized to everyone for harming them. He explained how they had worked all night to fix a virus but instead they had made a huge mistake. This video spread virally everywhere. But a funny thing happened. Instead of making things worse and getting sued, customers and partners became empathetic. The more the media tried to sensationalize it, the more empathy David and his team at McAfee received.

David ended up speaking to nearly every customer over the next few days. His office was flooded with calls from the White House, from state governors, from CEOs of many, many important companies. McAfee dispatched nearly 4,000 employees, and everyone worked together to fix the issue. Competitors piled on, but it only made things worse for them and not for McAfee. “Why hadn’t they fixed the virus themselves? Why hadn’t they worked as hard as McAfee did?” everyone was asking.

TURNING A HUGE NEGATIVE INTO AN EVEN BIGGER POSITIVE

By taking ownership and working with customers, you will lead by example.

Well, on that day, one of those companies was Intel Corp.: 70,000 computers wiped out. Employees had to stand in line in the cafeteria for days to get their computers fixed. Three days of being down. Well, Intel is an amazing company. Instead of being a victim, they took action, working with McAfee to design a semiconductor-based architecture to never let that happen again.

Three months later, not a single customer had sued McAfee. In fact, customers spent more money with them and their stock recovered, and a mere two months later, **Intel acquired McAfee for a record \$7.7 billion**, the largest all-cash transaction in the history of high tech. You see, David learned and continues to share this lesson with others – the most valuable of them all – Honesty.

Leadership lessons of life. Be present. Always alive. Live life on the edge of tears.

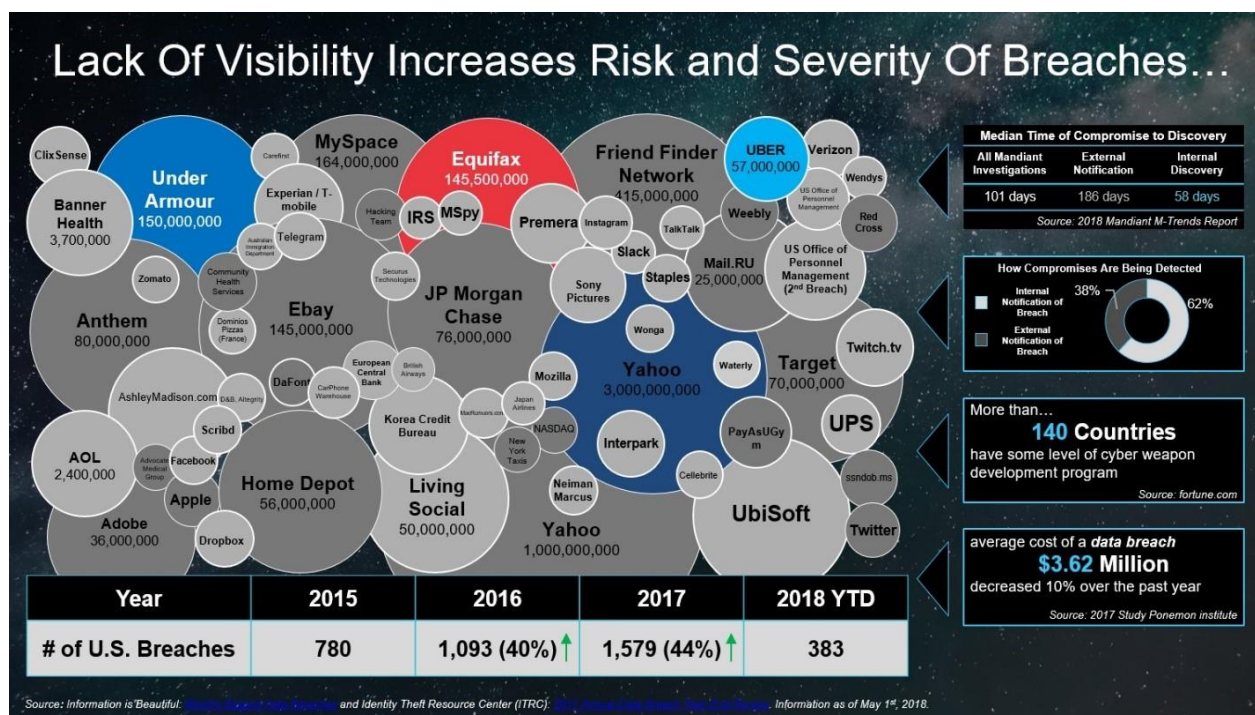
“Honesty — it’s a powerful attribute in a crisis. Hard-work, humility and honesty. The 3Hs are the foundation of my success,” said David DeWalt.

Many of you might remember how David DeWalt became CEO of Fireeye in 2012 and took it public in 2013. He and his team continued to build a multi-billion dollar valued business and even acquired Mandiant, whose founder, Kevin Mandia, is now running Fireeye. Today, Fireeye has revenues annually over \$300m and assets over \$2.5B.

SUMMING UP THE PAST, PREDICTING OUR CYBER DEFENSE FUTURE

Building out the first Cybersecurity Platform from Inception to Exit

So, Dr. David G. DeWalt has more than 30 years of experience in the industry – over 20 years in high tech and 17 years as a CEO, as he says “68 quarters of executive leadership has given me a front row seat – it’s my love, my passion – it’s not just a job – I feel lucky and blessed.” With these blessings and successes, Dr. David G. DeWalt has taken a bird’s eye view of what happened in the past, what’s happening today and predicting where we need to be in the very near future. His main driving concern is that the lack of visibility continues to dramatically increase the risk and severity of the breaches. This also opens up a new world of investment opportunities in cyber defense innovations.

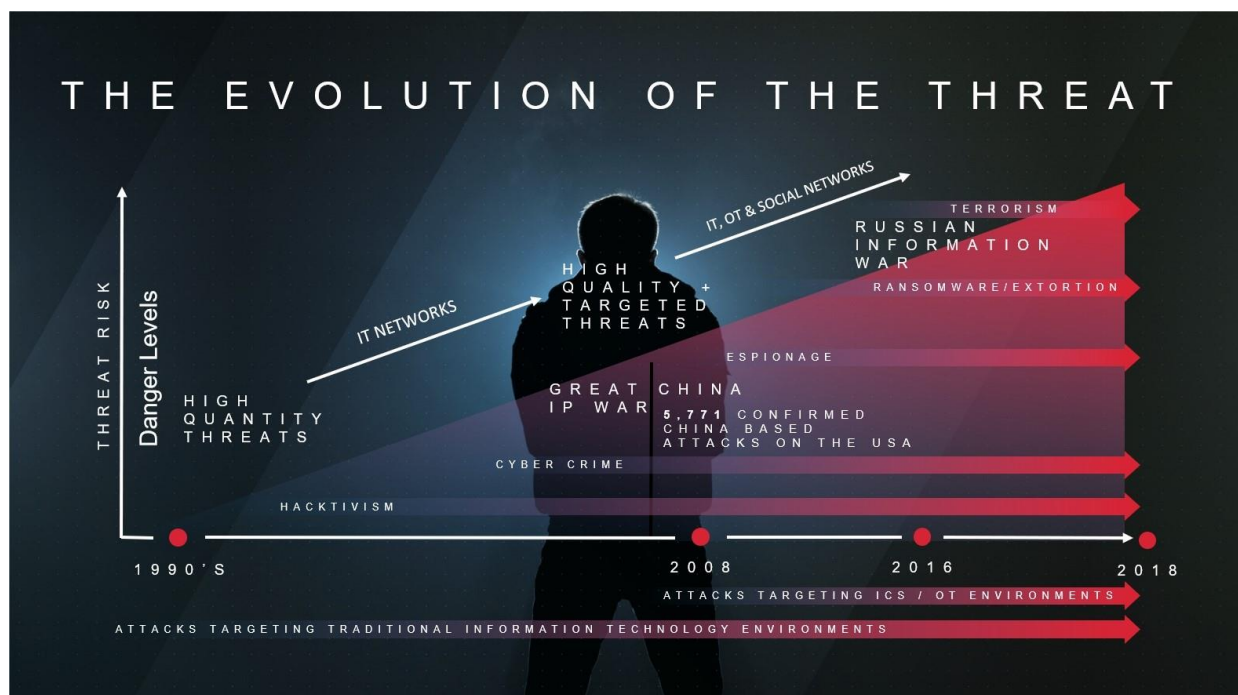


Pictured Above, Dr. David G. DeWalt's Thoughts On Greater Risk and Severity of Breaches

He's building out NightDragon Security (see: <http://www.nightdragon.com>) as a very innovative platform for cyber – a massive keiretsu of companies to make cyberspace a better, more secure and safe place for us all. Incubators – Team8 (see: <https://www.team8.vc/>) and DataTribe (see: <https://datatribe.com/>), new companies, a Venture Capital platform with one of my personal favorites, Bob Ackerman at Allegis Cyber (see <http://www.allegiscyber.com/>) and an amazing group of investment bankers and experts at M&A at MomentumCyber (see:<http://www.momentumcyber.com>).

WE'VE ENTERED THE PERFECT STORM IN CYBER DEFENSE

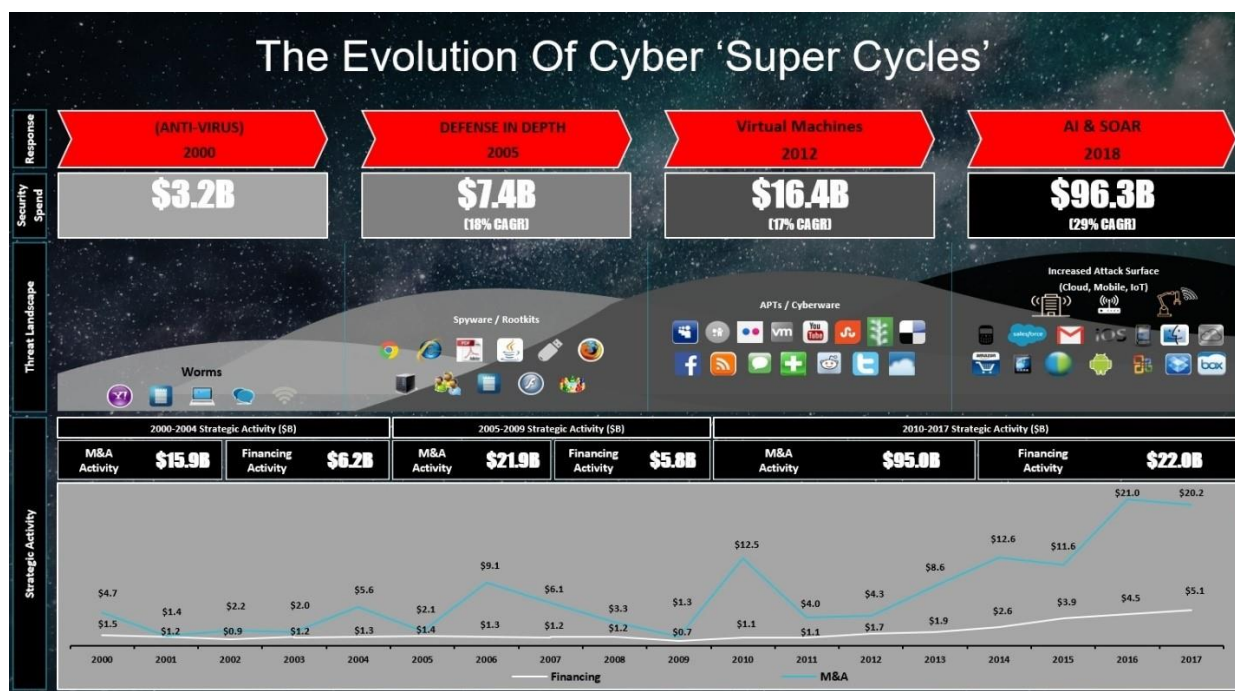
According to Dr. David G. DeWalt, with the biggest gaps comes the biggest investment opportunities, – if you see a threat, you will quickly see customer spend expand, then Venture Capitalists (VCs) pouring more money into those companies and of course it's cyclic, by the time the vendors solve it, the actors are onto new threats....



Pictured Above, Dr. David G. DeWalt's Threat Evolution from the '90's up to 2018

Dr. David G. DeWalt calls these "super cyber cycles" whereby these threat cycles drive vendor spending and investments, when he talks about biggest gaps, it's the offense or the threat vs commercial defense.

Wherever you see the biggest gap, it opens up to the biggest opportunities; Case in point: Fireeye. Along came the super threat cyber cycle in which advanced persistent threats (APTs) – multi-stage, attack vector, we'd never seen before and the antivirus (AV) vendors did not know how to stop 'all the objects.' "We took the risk at Fireeye and solved this challenge – we could tear apart APTs and understand their multi-object layering and multi-stages of behavior. I knew this would be a short, 3 year window – a big gap and a big opportunity – I see similar threat cycles coming our way and I call these Cyber 'Super Cycles'," said Dr. David G. DeWalt.



Pictured Above, Dr. David G. DeWalt's Idea of Cyber 'Super Cycles'

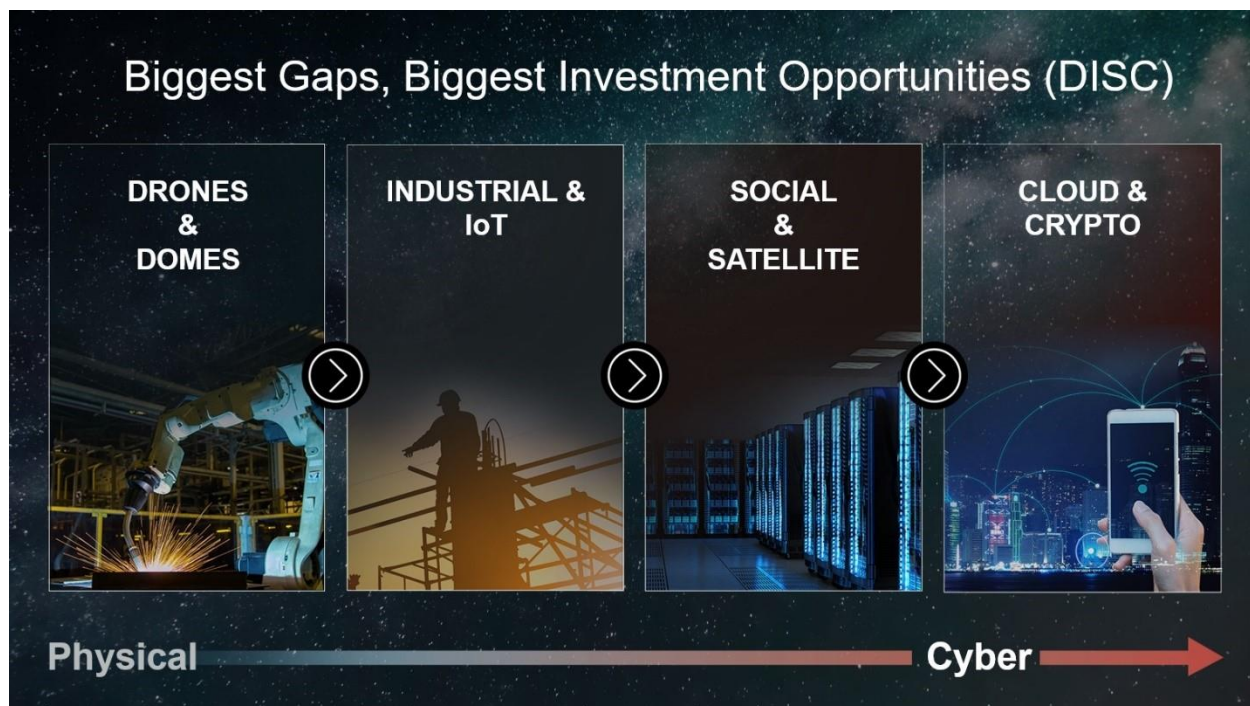
What's driving the perfect Cyber storm?

According to Dr. DeWalt, the speed of innovation is driving vulnerabilities everywhere, but in particular, eight key areas – Mobile, Social, Cloud, Satellite, IoT, Industrial, Physical, & Consumer. Add to this the levels of danger expanding from hacktivism to crime to espionage to terrorism to warfare. In addition, we have a tremendous increase in geopolitical tensions, a complete lack of governance and law enforcement models compounded by internet anonymity. Moreover, we have legacy security providers unable to detect or prevent the next threat – hence, we've entered a perfect Cyber storm.

A PERFECT STORM BRINGS A PERFECT OPPORTUNITY FOR INVESTING...

Given these critical issues, Dr. David G. DeWalt has decided to form NightDragon Security as a unique Cybersecurity Platform – to drive leadership into a new world of investment opportunities in cyber defense innovations. From inception to incubation to market deployment, acceptance and potential cyber defense global dominance – his mission is to create and/or find the market leaders to help us get one step ahead of the next breach. He's even predicting, very intelligently where those breaches will be happening – and you'd be very surprised. Today, it may be relatively easy to get to a CEO through a spear phishing attack but tomorrow, stealing his identity may happen through his home automation and internet of things (IoT) devices. Cybercriminals have already started

planning on moving from drive by malware found on websites to actually driving by (whether remotely through the internet or actually pulling a proximity attack) of an executive's property, eavesdropping on his or her insecure routers and weak home cybersecurity environment and making that the next big attack vector for cyber crime and espionage. Will the executive's Alexa or Nest system hold up to the scrutiny of cyber criminals or their 3-year-old wireless router that came with their cable modem? Highly doubtful. This is just one tiny example of what Dr. DeWalt has discovered. Let's read on and learn more from his key slide on the eight areas of high exploitation and high investment opportunity coming in the very near-term:



Pictured Above, Dr. David G. DeWalt's Cyber 'Super Cycles' Biggest Gaps Investment Vision

INVEST IN NEXT GENERATION DEFENSES

Drones & Domes, Industrial & IoT, Social & Satellite, Cloud & Crypto

Dr. David G. DeWalt suggests we go where there's incredible innovation in cyber and become part of that ecosystem and help these innovators commercialize and bring to market very next generation technologies that their respective government agencies might be using 'in the trenches' – so he's spent a lot of time in the hottest cyber locations – California, Washington DC and not surprisingly, Israel.

He went on to explain to me that NightDragon Security is not a corporation focused on one security issue, it's a complete platform to advance cyber across the world – taking these deep intelligence relationships and providing services necessary to cultivate them

from commercialization inception to incredibly significant and disruptive public offerings’.

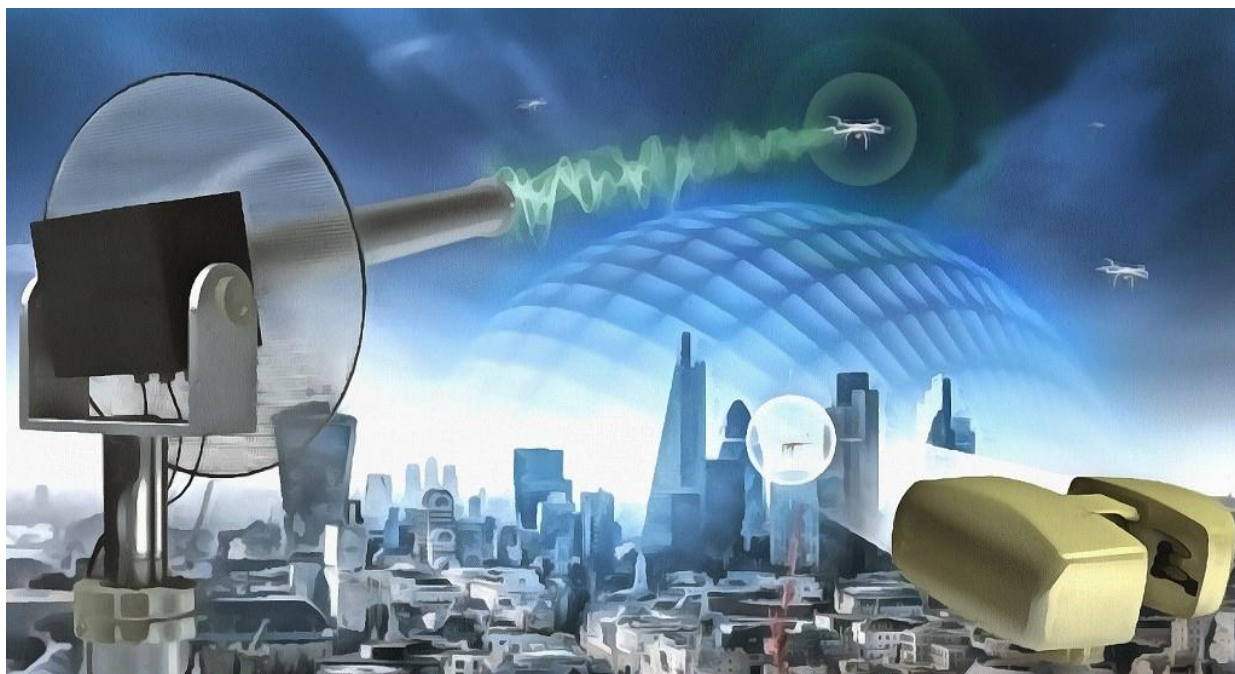
NightDragon Security is not looking to invest in ‘yet another endpoint’ solution or falling for the hype of ‘yet another a.i. solution’, it’s creating a unique platform for tomorrow’s solutions to come to market faster, to breath new life into a stale cyber defense economy. Yes, there are billions being spent on cyber security solutions but the problem he shares so honestly is that the exploiters have already begun shifting into these easily exploitable and very critical infrastructures. His teams’ mission is to take that knowledge and work with the future movers and shakers, the ‘Fireeye’s of the Drones dilemma or the Industrial ICS/SCADA area or the incredibly pervasive IoT area and the list goes on, as you can see from his Biggest Gap slide. So let’s go through these and learn from him how the future will play out in Cyber Defense, shall we?

DRONES & DOMES

These are two separate categories but also very similar, with one driving the other...

In the case of **Drones**, how do we have a perfect Cyber storm? According to Dr. DeWalt, the number and types of drones is growing incredibly – their speed, performance (improvements in batteries using carbon nano-fiber tech, etc.) the technology is moving much faster than any thoughts about security. These devices have lots of vulnerabilities and because of this explosive innovation, have also created a very large attack surface.

They will soon deliver packages and baggage and soon – people. But what happens when a drone, heaven forbid, is carrying explosives? **Or what happens when a drone becomes armed and learns how to ‘shoot to kill’?** With beehives and base stations for management of deliveries and the usage of drones outside of the military, we now have enabled the opportunity for very bad actors – cyberterrorists, hacktivists and cybercriminals to attack innocent civilians, steal information and even hold you hostage with ransomware that might hit your package delivery fleet. There are so many scenarios it creates the need for drone hardening, drone protection as well as drone intrusion detection and prevention. Therefore, NightDragon Security will be making investments in this space. In addition, Dr. DeWalt sees the need for Domes because of Drones.



Pictured above, rendering of a future dome and EMP (DDoS) defenses against drones

Would you keep a blacklist of bad drones and track anomalous behavior “like Fireeye’ and then block ‘like a firewall’ – some form of antenna-based deep packet inspection and prevent a hijacked or malicious drone from entering your ‘cyber dome’? The answer is yes, and this new arena is also getting incubated by NightDragon Security. Cyberdomes will prevent all kinds of threats in the dome.

Dr. DeWalt predicts that there will ultimately be cyber **Domes** over every physical space, protecting against multiple threat vectors – such as satellites taking pictures on or to listening to people talking to drones also eavesdropping. The future of cyber domes will be to detect and prevent – monitor, good vs bad, ultimately to protect the area above your physical fence – air spaces above will need the same form of cyber protection that physical spaces have, below. He shared ideas about not only high tech commercial usage and military usage but even those involved in the movement of trucks, packages, crop growth – anything that can be spied upon by a drone will need some form of a dome.

INDUSTRIAL & IoT

These are two other very interesting areas that are extremely vulnerable...

In the **Industrial** arena we have ICS and SCADA equipment helping manage everything from railroad tracks to water, power – from coal to natural gas to nuclear power to manufacturing with so many proprietary and insecure protocols – it’s a wonder this industry is not experiencing more Stuxnet-like attacks. Dr. David G. DeWalt asked me to ‘name one security solution designed to monitor Rockwell or Honeywell PLC’s’ and for

once I was stumped. He brought up the critical infrastructure issue right now that cyber criminals and cyber terrorists going on the offense have massive advantage by implanting capabilities into these networks using the art of cyber war and you could, heaven forbid, bring down US critical infrastructure. These industrial networks are desperately in need of another "Fireeye" like solution and Dr. DeWalt is 'on it'. Stay tuned for more in this industry. I am impressed with TemperedNetworks (see:<http://www.temperednetworks.com/>) , CryptoniteNxt (see:<https://www.cryptonitenxt.com>) and Owl Cyber Defense (see:<https://www.owlcyberdefense.com/>) with their unique approaches to helping solve this problem with 'zero-trust' and Dr. DeWalt says there will be more coming – with a potential multi-billion dollar valued company in this marketplace very soon.



Pictured above, one of the many high risk Industrial SCADA gas energy facilities

The **Internet of Things (IoT)**. Many people call these devices 'smart' devices. Both Dr. DeWalt and I are replacing the word 'smart' with 'extremely vulnerable' – there are way too many IoT devices connecting to IP networks vs industrial networks: from your Nest or similar thermostats on your home or business wifi to smoke alarms, smart-locks, door-bells with cameras to so many more. The consumerization of IoT home and office seems amazing and enabling yet, most of these devices are extremely vulnerable – it's almost as if each vendor either rushed them to market with accidental vulnerabilities or some of them have purposeful built-in backdoors.



Pictured above, the plethora of Internet of Things (IoT) devices with more to come

Either way, we have a plethora of Trojan-horses masquerading as innovative and productivity enhancing devices yet most of them are just waiting to be exploited. I hate to digress, but I was recently speaking at InfoSec Manchester in the UK and one of the speakers hacked devices we can't write about in our magazine and showed how he found some important individuals using these devices by eavesdropping on wifi (think <https://www.shodan.io/> for embarrassing IoT devices...need I say more?). These are the kinds of IoT devices you won't write home to mom about. He even showed a web site with a search engine for them. His name is Ken Munro at PenTestPartners (see: <https://www.pentestpartners.com/>) but this just confirms Dr. DeWalt's suspicions – that your home IoT is a big back door to exploiting you – and if you are a C level executive at a major corporation, what better way to steal your identity, by riding the vulnerabilities of your internet of things. Dr. DeWalt also believes we will see major investments in vulnerability management and intrusion detection and prevention for IoT. Makes so much sense when you think about it.

SOCIAL & SATELLITE

Billions have shifted from Email to Social Media and Satellites Connect Us Globally

There are nearly four billion people on **Social Media** networks, daily – that's nearly half of all humanity. The issues in this area range from false identities (see: <https://www.cbsnews.com/news/facebook-scams-when-your-friends-are-actually-hackers/>) to the huge regulatory compliance issues impacting Facebook and

others now that GDPR is being activated. There are stories that the Russian government funded an organization that only spent \$100k to influence, potentially 10M voters and the list goes on. The first stage of any form of cyber security in this area is better cyber hygiene – most folks don't even know what apps have access to all of their personal information in their social media accounts. But where is the 2-factor authentication – how do we know a Twitter, Facebook, LinkedIn, Google+, Instagram or other social media account is really YOUR account? What if you had a false identity in any other country and didn't know it? What if your staff were victimized by one of these false identity accounts? Social media has little to no cybersecurity by design. How do we manage, monitor, prevent and protect when it comes to cybercrime, false identities, online extortion and the next wave of e-commerce threats that leverage these weak and insecure platforms vs traditional ecommerce web experiences?



Pictured above, social media is beginning to takeover and replace the web

Most industries and even consumers have become completely dependent upon **Satellites** and don't even think about it or even notice – from connecting everything on the ground to the air – internet is provided now on most major airlines and rural communities leverage satellite for internet but there's so much more – think of all the smartphones and IoT devices – even cars, trucks, air lines and shipping industries using GPS – all based upon weak and insecure satellite networks. Satellites are hard to upgrade, have very weak and old encryption, can be easily Distributed Denial of Service (DDoS) and so much more – this area is ripe for investment and innovation in cyber defense, according to Dr. DeWalt. There's only one company, to date, putting in any energy into

satellite security, whereas there are over 50 antivirus vendors and a dozen firewall vendors. This is a completely insecure, yet critical market in need of a solution.



Pictured above, high risk satellites with very weak encryption and easy to DDoS

CLOUD & CRYPTO

Everyone uses the cloud from B2C to B2B and everyone will be using Crypto

Ask anyone who hasn't heard of DropBox or Salesforce? But as Dr. DeWalt clearly pointed out, ask the typical CISO how many cloud-based apps there are running in their enterprise and they will tell you 42 when they are actually running 928. There's no proper hygiene when it comes to identity and access management (IAM) in the cloud, onboarding and offboarding of users, understanding the security capabilities and defenses for each of these 928 cloud SaaS apps and the list goes on. We're looking at a very insecure market sector in need of innovators. Both Dr. DeWalt and I have found some such as Cyren (see: <https://www.cyren.com/>) and Dome9 (see: <http://www.dome9.com>) as well as ThreatStack (see: <http://www.threatstack.com>) to SourceDefense (see: <https://www.sourcedefense.com/>) to SkyHigh Networks (see: <https://www.skyhighnetworks.com/>) to Defiant (see: <https://www.defiant.com/>) and others. This has become the 'obvious' area to make cybersecurity investments so Dr. DeWalt is making more advanced investments in areas here that he feels will solve tomorrow's cloud problems, today. Some of these players will end up with billions of dollars in valuation with little to no revenues. Stay tuned as we continue to explore this area....



Pictured above, the cloud needs security and so does bitcoins and blockchains

I was thrilled to talk with Dr. DeWalt about the **Crypto** area (not strong encryption, which is also an area of great interest to me) but about crypto currencies and blockchain-based technologies. One of the reasons is I have a book coming out this year on this subject matter so we had much to discuss here, however, as my book will show you, the two of us could put together hundreds of pages on this subject matter alone. We discussed some of the amazing advances such as Ripple becoming a potential replacement for the highly hackable SWIFT payment gateway system. We also both agreed that there are some big questions beyond performance – how is Ripple secure? Has the code been vetted by systems like WhiteHatSec (see: <http://www.whitehatsecurity.com>)? Let's face it, we're only a few years away from every single person having an opportunity to leverage crypto as a potential e-commerce, wallet, currency and credit card replacement. That has opened up major opportunities for cybercriminals beyond the WannaCry's of the world, where ransomware leverages crypto solely for payments. On top of that, we have every major industry from health care to real estate to insurance to banking all claiming they are jumping on the Blockchain bandwagon but without any major infosec solutions available to help them secure the process. This will be a very hot area for billions in valuations and IPOs in the near future.

So, there you have it. We've covered the eight very hot areas and some great predictions from a super bright, successful, talented and passionate market leader. Keep an eye on NightDragon Security to see how this market will shake out.

MOVING THE CYBER DEFENSE MARKETPLACE FORWARD AT LIGHT-SPEED

With Great Opportunity comes Great Risk – Both for Failure and Success

The essence of Dr. DeWalt's vision for NightDragon Security – create a platform to find the means and methods to accelerate getting cyber defense solutions out there more quickly that will close the huge gap in these eight critical areas of networking, while of course, capitalizing on it at the same time – creating many jobs and wealth. It's a win-win scenario and the **NightDragon Security train is already leaving the station** at bullet-train speed. *No, make that light-speed!*



Pictured above, we are just now at the tip of the iceberg in these eight key areas...

THIS WHITEPAPER IS ONLY THE TIP OF THE ICEBERG

We have so much more to cover and to learn from Dr. DeWalt so stick around...

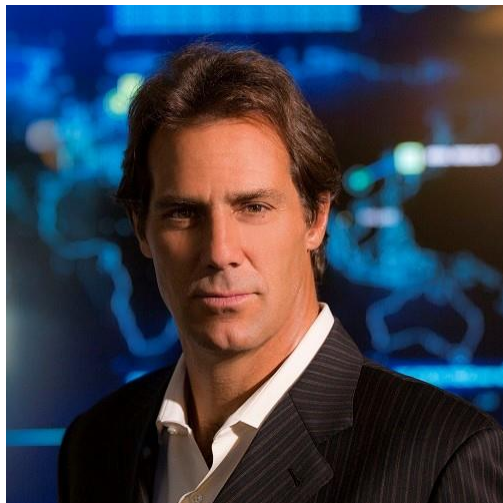
Remember, we're learning from someone who not only built out amazing high tech and cyber security companies, he's been actively helping one of the largest air lines in the world. Delta Air Lines owns oil refineries, consumer air transportation, military transports, mechanical repair businesses and so much more that he's been able to learn things from the customer side of the fence, as well. Most cyber security CEO's never get this kind of opportunity. He's seen and heard all the stories in the trenches. He understands, for example, that the average CISO will tell you they have 42 cloud apps but after careful analysis, they find out they have 928. Just let that sink in for a moment! He's helped oversee the security of Delta.com – a tiny website, right? How about a \$20B online commerce business? How about the social media aspect where the next generation is buying their airline tickets on Facebook (from Delta's Facebook experience – they may never visit the dot com). Think about it? We're learning from a humble leader who has a

treasure trove of knowledge to share and unfold. I know it can't all happen in this one article or a day's time but know this – it's happening and he's willing to continue to share these insights with all of us. InfoSec Knowledge is Power and we're going to get a lot of it, thankfully, from Dr. DeWalt's willingness to share.



Pictured Above, The NightDragon Security Keiretsu, and this is only the beginning...

About David G. DeWalt Ph.D.



Dr. David G. DeWalt, Founder of NightDragon Security at <http://www.nightdragon.com>. He

most recently served as the Executive Chairman of FireEye, Inc., a global network cyber security company. Dr. David G. DeWalt served as FireEye's Chief Executive Officer from November 2012 to June 2016 and Chairman of the Board from June 2012 to January 2017. Dr. David G. DeWalt was President and Chief Executive Officer of McAfee, Inc., a security technology company, from 2007 until 2011 when McAfee, Inc. was acquired by Intel Corporation. From 2003 to 2007, Dr. David G. DeWalt held executive positions with EMC Corporation, a provider of information infrastructure technology and

solutions, including serving as Executive Vice President and President-Customer Operations and Content Management Software. Qualifications: Dr. David G. DeWalt has substantial expertise in the information technology security industry and has strategic and operational experience as the

former Chief Executive Officer of FireEye, Inc. and former Chief Executive Officer of McAfee, Inc. As a member of the boards of directors of public companies other than Delta, Dr. David G. DeWalt has served on the audit and compensation committees. Directorships: Five9, Inc.; Forescout Technologies, Inc.; FireEye, Inc. (2012-2017); Jive Software, Inc. (2011-2013); Polycom Inc. (2005-2013) Affiliations: National Security & Technology Advisory Committee. Learn more about Dr. DeWalt at <http://www.nightdragon.com> and <https://www.linkedin.com/in/ddewalt/>

About the Author



Gary Miliefsky, Publisher, Cyber Defense Magazine

Gary is our Publisher and a globally recognized cybersecurity expert, speaker and keynote, investor, advisor and consultant. He is the inventor and founder of technologies and corporations sold and/or licensed to Hexis Cyber, WatchGuard, Intel/McAfee, IBM, Computer Associates and BlackBox Corporation. He is currently the CEO of Cyber Defense Media Group (CDMG), which is the Publisher of Cyber Defense Magazine and Cyber Defense TV, is a frequent invited guest on national and international media commenting on mobile privacy, cyber security, cybercrime and cyber terrorism, also covered in

Inc, Forbes and Fortune Magazines. Miliefsky is a Founding Member of the US Department of Homeland Security (<http://www.DHS.gov>), the National Information Security Group (<http://www.NAISG.org>) and the OVAL advisory board of MITRE responsible for the CVE Program (<http://CVE.mitre.org>). He also assisted the National Infrastructure Advisory Council (NIAC), which operates within the U.S. Department of Homeland Security, in their development of The National Strategy to Secure Cyberspace as well as the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. Gary is a member of ISC2.org and is a CISSP®. Learn more about him at <http://www.cyberdefensemagazine.com/about-our-founder/>

BONUS TAKEAWAY TO SHARE WITH YOU

One lesson I will share with you, personally, from listening to Dr. DeWalt is this – I've built and sold startups, I've spent many years at the whiteboard, working on patents – being trained by Wang Labs to believe at all costs, protect the intellectual property. I remember Wang Labs patent attorney literally saving our company by getting a \$100M agreement in place with Microsoft over our invention at Wang – Object Linking and Embedding (OLE, which became ActiveX). That kept the lights on for us for 6 months at the darkest hours of Wang's amazing history. But that's all that it did. What Dr. DeWalt said that stuck to me like glue, personally, is "Intellectual Property – IP portfolio development is a game of inches. Execution is a game of miles." Remember this – it's better to focus on how to grow, sell, manage, distribute and create profit, than to spend precious cycles on developing an IP portfolio that will ultimately only become valuable to lawyers.

