Four Imperatives for Cybersecurity Success in the Digital Age: We Must Flip the Scales

Major General John Davis, USA, Ret

PART ONE OF A FOUR PART SERIES*

Having joined Palo Alto Networks following a 35-year career in the U.S. Army, the past decade of which I served in a variety of leadership positions in cyber operations, strategy and policy, I have found that many of the cybersecurity challenges we face from a national security perspective are the same in the broader international business world.

This article and the companion posts in The Cyber Defense Review Blog describe what I consider to be four major imperatives for cybersecurity success in the digital age, regardless of whether your organization is a part of the public or private sector.*

To provide a sense of what I intend to cover in this series, here are the major themes for each imperative:

- Imperative 1 – We Must Flip the Scales
- Imperative 2 – We Must Broaden Our Focus to Sharpen Our Actions
- Imperative 3 – We Must Change Our Approach
- Imperative 4 – We Must Work Together

ARTICLE 1 OF 4: IMPERATIVE 1: WE MUST FLIP THE SCALES

This first article in the series covers Imperative 1 for cybersecurity success in the digital age. Before I get to the details of the first imperative, allow me to provide some background and context for all four imperatives, and then I'll provide an executive summary of the first imperative.

**Part Two, Three and Four of this series will be published on The Cyber Defense Review Blog at http://www.cyberdefensereview.org/blogs/.*

Retired U.S. Army Major General John Davis is the Vice President and Federal Chief Security Officer for Palo Alto Networks, where he is responsible for expanding cybersecurity initiatives and global policy for the international public sector and assisting governments around the world to successfully prevent cyber breaches.

Prior to joining Palo Alto Networks, Major General Davis served as the Senior Military Advisor for Cyber to the Under Secretary of Defense for Policy and served as the Acting Deputy Assistant Secretary of Defense for Cyber Policy. Prior to this assignment, he served in multiple leadership positions in special operations, cyber, and information operations. His military decorations include the Defense Superior Service Medal, Legion of Merit, and the Bronze Star Medal.

Major General Davis earned a Master of Strategic Studies from the U.S. Army War College, Master of Military Art and Science from U.S. Army Command and General Staff College, and Bachelor of Science from U.S. Military Academy at West Point.

BACKGROUND AND CONTEXT

First, my role as the Federal CSO for Palo Alto Networks requires that I *evangelize* to the various groups of individuals, leaders, and organizations with which I interact. My job is to use my experience to ensure a deeper understanding of the cyberthreat landscape, and provide thought leadership about useful concepts to deal with a growing threat while ensuring that leaders can manage risk in ways that enable their business or mission.

Second, because of my military experience, I think of effective ***concepts*** regarding several key factors. I use these factors to explain concepts in a comprehensive way to describe each of the imperatives for cybersecurity success in the digital age. Figure 1 below provides the four factors that I use.

THREAT
This factor describes how the evolving cyberthreat and the response to those changes.

POLICY AND STRATEGY
Given our assessment of the overall environment, this factor describes what we should be doing, and our strategy to align means **(resources and capabilities–or the what)** and ways **(methods, priorities and operations–or the how)** to achieve ends **(goals and objectives–or the why).**

STRUCTURE
This factor includes both organizational (human dimension) and architectural (technical dimension).

TACTICS, TECHNIQUES AND PROCEDURES (TTP)
This factor represents the tactical aspects of how we actually implement change where the rubber meets the road.

Figure 1.

My last point of background and context is about the digital age, itself. So, what does the digital age environment look like? Two significant trends I would like to cover.

First, our growing societal reliance on technology for just about everything we do is only going to increase. This is not news to anyone; and, regardless of whether you are talking about public or private organizations or personal lives, there is no escaping the level of trust that we continue to place in technology. Equally increasing is the level of human connectivity, and in the devices we use to do almost everything in our daily lives. The phenomenon of the Internet of Things represents this trend.

The second trend is not news to anyone either. Just look at the growing list of headlines regarding cyber breaches across government and industry worldwide. Figure 2. depicts the most recent list of cyber breaches—it's a mess! I believe it's going to get worse before it gets better. You've all heard the tired (but, nonetheless, true) saying, "It's not a matter of if, but when." The trend is alarming; and, regardless of whether you sit in the public or private sector, you must recognize that the cyberthreat is a serious problem, representing an ***imperative for change*** if we are going to be able to continue to place trust in the opportunity the digital age promises.

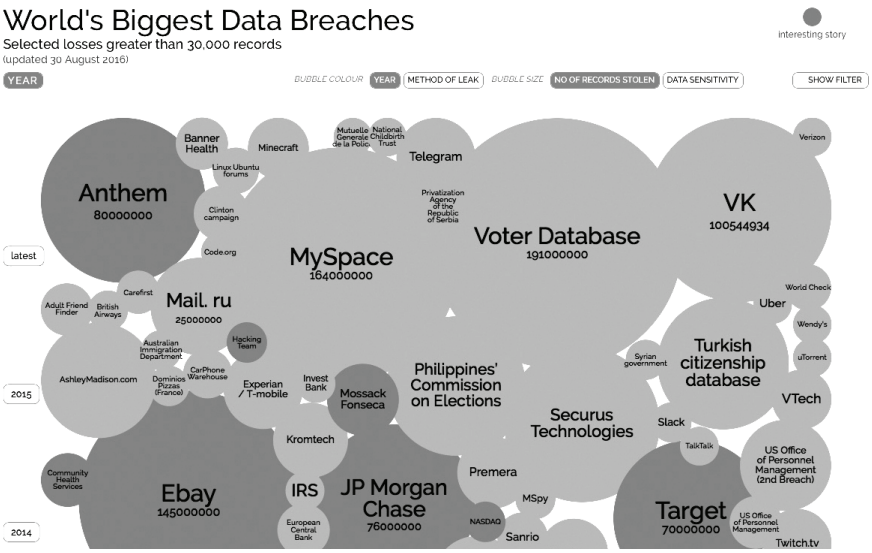

Figure 2. Source: http://www.informationisbeautiful.net

Using Figure 3. as a reference, we must *flip the scales*, or at least rebalance them, to improve the cybersecurity posture that we choose to live with today. Using the concept model below, I step through the implications via the categories of Threat, Policy and Strategy, Organizational and Architectural Structure, and finally Tactics, Techniques and Procedures (or TTP).

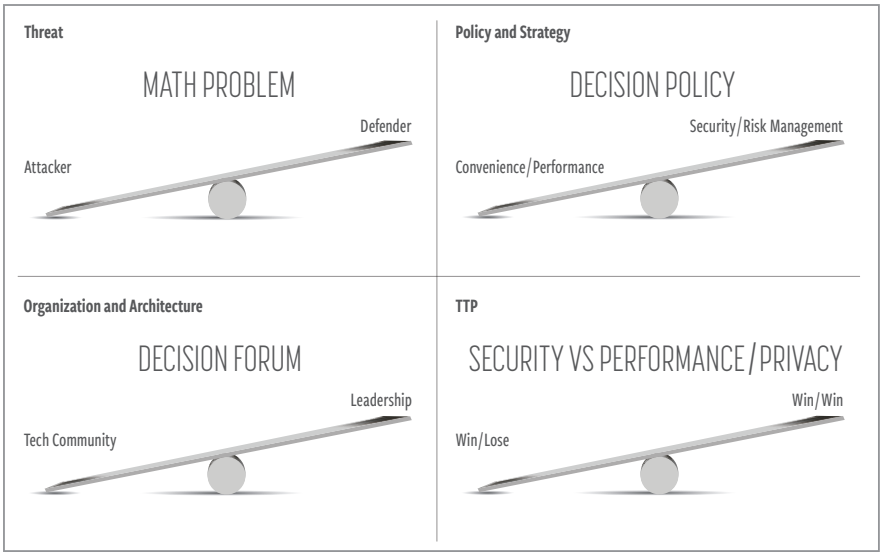

Figure 3.

EXECUTIVE SUMMARY

We have a math problem that is giving today's cyberthreats a significant advantage over our ability to secure and defend our networks. This issue pits a growing adversary marketplace—that leverages information sharing, automation and the cloud at increasing speed and decreasing costs—against the cybersecurity community, which is slow, clumsy, largely manual and increasingly expensive.

Part of the reason we have this math problem is due to legacy thinking and resulting policies that heavily favor opportunity and convenience over security and risk management rather than a more balanced approach toward both. Flipping the policy scale from a *trust everything* to a Zero Trust model ("never trust, always verify") will help to flip the scales on the attacker/defender math problem.

To change the policy balance and drive a real strategy that aligns limited resources and methods to achieve results also requires leaders to enter the decision-making forum for cybersecurity. A successful organization enables leadership to make decisions through collaboration between their IT and cybersecurity experts, working in tandem to provide precise, accurate and clear recommendations. This is how the leadership of an organization can drive successful policy and strategy. It is also how the leadership and tech teams should work toward common goals and routinely demonstrate progress with real, measurable results.

Finally, cybersecurity success in the digital age requires a new way of thinking about our TTP. Implementing real change needs rebalancing performance and security together, just as we also rebalance security and privacy together, empowering IT and cybersecurity teams to partner in a win-win dynamic, rather than pitting one community against the other with win-lose priorities. This is how an organization can go about safely enabling the high performance of its users, using the applications and content the organization requires to do its vital functions, including fixed, mobile and virtual capabilities throughout the organization's enterprise, from the cloud to the network to the endpoint device—BYOD or otherwise.

DETAILED DESCRIPTION OF IMPERATIVE 1

THREAT: Looking at this concept from a threat perspective, we all know that, today, the Attacker has a distinct advantage over the Defender. That's not news, and we all know that; but let's look at why that is true, and why cybersecurity will deteriorate unless we do something to *flip the scales*, or at least rebalance them toward a better security posture.

Our CEO at Palo Alto Networks, Mark McLaughlin, calls it a math problem. Due to the decreasing cost of automation and cloud-based capabilities, a growing marketplace of threat actor information sharing, and the ever-increasing attack surface with vulnerabilities growing in proportion due to the "Internet of Things" phenomenon, the Attacker's job is getting cheaper and easier every day. The Attacker only has to be successful once to get

into your network and accomplish their nefarious objectives.

On the other hand, the Defender has to be everywhere, all the time. Additionally, the Defender, who typically uses manual procedures to respond, does not usually detect the threat in their networks until months or even years have passed. The average detection time is more than six months according to most cyberthreat research and analysis. This is very costly in terms of time, manpower, technology, complexity, reputation, brand, and, of course, money.

To illustrate further, I would like to use a few numbers to tell a story about the world of protecting your business from cyberattacks and this math problem. These numbers from our Regional Chief Security Officer (CSO) for Europe and the Middle East, Greg Day. In 2015, the Application Usage Threat Report from Palo Alto Networks saw 675,000 distinct threats, across almost 3000 applications. These are frightening statistics. But what does this mean in real terms to your business, to your team, or to you personally? To get a feel for that kind of meaning, you need a context that's relevant to your environment, so let me give you another number—1.5 million.cAccording to analysts Frost and Sullivan, this will be the shortfall of cybersecurity professionals by 2020.

This demand outstripping supply is good news if you're a security professional looking for a job, but bad news if you are trying to recruit cybersecurity professionals into your organization or retain your existing workforce. Many organizations have a model that is becoming harder and harder to sustain in this global environment of more threats and less security staff at the ready.

Implementing real change requires rebalancing performance and security together.

Who are these Defenders? The Chief Information Security Officer (CISO) and other IT security professionals defend their organization—against what, though? Today, it's not just an attacker; it's a marketplace, and that means groups of people sharing best practices with each other. A few years ago various governments were investing huge amounts of resources in developing incredibly sophisticated attack approaches. Today, anyone can purchase the same attack kit online for a few dollars, complete with instructions, and a how-to-get-started video.

This is why it's getting easier for Attackers, because of their decreasing costs and the abundance of resources available to them. They only have to be successful once to win, but this is probably a tiny percentage of their attack attempts. Contrast that with the CISO, who has to defend 100 percent of the time successfully. Attackers are crowdsourcing, yet CISOs are on their own.

I will demonstrate in the following sections of the concept model, how many leaders and security professionals are taking action to alter their defensive model to take advantage

of the valuable assets they already have in *flipping the scales* to give the Defender more of an advantage than they have today.

POLICY: The legacy view is that opportunity and convenience drive technology (which are built-in) while security and risk management chase from behind trying to catch up (and are, therefore, bolted-on afterward).

The environment, as shown in Figure 2 above and captured in daily headlines about the latest breaches, is changing this balance; but the change is slow and uneven. This shift is beginning to bring the scales in Figure 3 to a more responsible balance. This includes changing a *left side of the scale* assumption that you are safe, to a *right side of the scale* assumption that the threat is going to get in, if it has not already, resulting in the need for a Zero Trust environment.

Security leaders want to reduce the workload on their organization. Getting back to our earlier math problem, here's another number—65,000. This figure comes from Greg Day, and identifies some of the reasons the network defender's workload is so big. When the Internet was conceived, that was the number of ports of communication that people thought might be needed for all the different traffic and protocols. This provided lots of scope and scale for flexibility. Today, we use very few of these traditional ports. Most of the traffic consists of either email or web-based protocols; however, within these, there are now thousands of Internet applications, and each has its own sub-protocols. You can block all these ports; but, since almost all the traffic comes through these same few ports, you cannot just block them. Using traditional technology, you have to trust these ports or block out all the traffic needed to run your business.

> The Attacker has to only be successful once to get into your network and accomplish their nefarious objectives.

This policy means that security professionals have to program their legacy firewalls to block traffic using rules that are based on where traffic is coming from, where it's going to, and what type of traffic. And, of course, your organization wants to do new things all the time, so the policies have to change frequently. Your starting position is to trust all the traffic going through these few ports. Then you have to block traffic using policies—lots of policies. Policies on top of policies. Rules on top of rules. It's very difficult to even understand what the policies and rules of the past accomplished, and if the new policies and rules conflict in any way. This approach is costly, labor-intensive, and ineffective because it's using this old frame of reference that only adds complexity and cost to the equation, neither of which are your friends as a cybersecurity professional.

The only correction is to design a totally new type of technology using a different frame of reference based on how we use the Internet today. You need technology that under-

stands modern Internet usage and identifies each of the applications that effectively uses its own protocols over the few trusted ports each business has enabled today. This is exactly why our tech industry is engineering next-generation firewalls to safely enable the applications and content required by an organization's users, whether fixed, mobile or virtual, to do the vital functions required for the mission or business.

The balance on the right side of the policy scale is called a Zero Trust model. Trust nothing unless it is defined as part of how you operate your business. This essential capability is unique. It also allows you to create rules that determine what traffic can flow into your organization. But, instead of being based on the port, the type of traffic, where it's from, and where it's going to, it's based on who wants to communicate, and what they want to do. That means the applications and content they want to use.

The result is that it's easy to define your company's way of doing business because of fewer policies, which are relevant to how your organization operates. They also make sense, and you can see your security policy written in black and white. It's more effective because your starting point is Zero Trust rather than trust everything, and it understands the sub-protocols that modern web applications use. It's easy to follow and much less work.

ORGANIZATION: The decision-making forum when it comes to dealing with cyberthreats has traditionally been within the technical (CIO/CISO/CSO) community, but the exploding threat challenge along with the changing balance between opportunity/convenience and risk are driving the decision-making forums into C-Suites and boardrooms; no longer the sole purview of the IT community. This is becoming more and more a leadership issue rather than just a technical concern. So this scale has already begun to flip, and that's a good thing!

Leadership is the most critical aspect of this imperative to change the balance and create an environment where those in the business of driving cybersecurity within an organization can begin to acquire an advantage over the threat. Leadership from the top drives the prioritization of resources and assets, enables an effective strategy that aligns the ways and means to achieve real goals, and requires the team to routinely bring back results that can be measured in relationship to the bottom line, whether you are a business or a national security organization.

This changing balance within the decision-making forum in no way diminishes the role of the technical community in the overall decision process. The tech community must take greater care than ever before to educate their leadership in clear, accurate ways so that sound decision-making is the result. Not all senior executives have the technical background to readily comprehend the details required to address what can be a very mysterious and complex problem set. It's incumbent on the leader's technical experts to explain issues in plain English to the maximum extent possible.

The technology environment associated with cyberspace has some of the most significant distinctions when compared to the traditional physical 'domains.' Scale, speed, and complexity (especially given the blurring of lines between human interaction with cyberspace and the various layers of technical, logical, physical and geographic segments) make analogies dangerous because, inevitably, the analogy falls apart at some point, and senior executives who think they understand what decision to make based on an imprecise analogy can be making serious mistakes.

TTP: So why does it seem we continue to lose, and the problem is deteriorating and not improving? Why haven't we all had a *Cyber Pearl Harbor* or *Cyber 9/11* epiphany? From what I can see, it's because there is still a false narrative about the balance between security and performance; that you can only increase one at the expense of the other. This traditionally describes a win-lose dynamic. In the world of business just as in the world of national and economic security, performance always wins, which is why most CISOs report to the Chief Information Officer (CIO). And when they do not, it's always a win-lose proposition pitting one community against another.

This is why it's getting easier for Attackers, because of their decreasing costs and the abundance of resources available to them.

In this new environment, security and performance go hand-in-hand, so how do we enable a *win-win* dynamic? How do we put security into a model that safely and effectively *enables* performance, across all users, using all their applications, all their content, including mobile and virtual devices? Is that even possible? If your cybersecurity solution provider isn't working toward that objective, shouldn't they be?

In the above threat discussion, organizations are faced with the attacker having low costs and automation requirements, and the defender has high costs and humans performing manual tasks. This is why leaders are looking for another solution because this model is difficult to sustain. Perhaps it is even unsustainable.

Imagine if you could change the balance. At the moment, this precious resource—your staff—is focused primarily on discovery. Taking productive business action is secondary. This model gives a poor return. What if your people only took productive business action and the discovery part was automated? That model would give you a much higher return. More on manual vs. automated in one of my next *CDR* Blog posts about other imperatives for cybersecurity success in the digital age.

Helping us to pursue a win-win dynamic is to speak with more clarity and accuracy about what we are trying to do with information sharing to provide cybersecurity and

distinguish that from some of today's conflated ideas about providing *traditional* security and the associated *surveillance* issues that get carelessly lumped into cybersecurity discussions.

In addition to the false narrative about performance vs. security, I think there's another false narrative regarding security vs. privacy. In the cybersecurity world, unlike the world of counterterrorism and surveillance issues, security ensures privacy; it doesn't detract from it! For example, we should begin to clearly identify exactly what kind of cyberthreat information needs to be shared, and how a narrow focus on that specific information has little (or maybe even nothing) to do with privacy-related information.

I will cover more about information sharing in Imperative 4; but, for now, let me summarize the key tenets of this first imperative about *flipping the scales.*

CONCLUSION

Cybersecurity success in the digital age requires immediate action to change several important dynamics that are currently out of balance. Legacy thinking and resulting policies put the cybersecurity community on the wrong side of a math problem when it comes to the threat, and in a win-lose dynamic with both the IT community and our leadership when it comes to choosing between performance and security. We have to *flip these scales,* with organizational leadership driving this effort accompanied by active IT participation, and cybersecurity communities working toward common goals.

We also need to start throwing the weight of our technology, processes, and people on the side of the scales, favoring next-generation technology that recognizes how the Internet works today, leverages the powerful advantage that automation brings to discovering threats on a wider scale, and in reduced time, and saves our most precious resource—our people—to do what only people can do instead of spending all of our resources in "cleanup on aisle 9" mode.

Next in the online *CDR,* our series continues with Imperative 2 for cybersecurity success in the digital age: ***We Must Broaden Our Focus in Order to Sharpen Our Actions.***