THE DIGITAL BIG BANG

THE HARD STUFF, THE SOFT STUFF, AND THE FUTURE OF CYBERSECURITY

PHIL QUADE
CISO, FORTINET

WILEY

the DIGITAL BIG BANG

THE HARD STUFF, THE SOFT STUFF, AND THE FUTURE OF CYBERSECURITY

Phil Quade, CISO, Fortinet

WILEY

The Digital Bing Bang: The Hard Stuff, the Soft Stuff, and the Future of Cybersecurity

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published simultaneously in Canada

ISBN: 978-1-119-61736-5
ISBN: 978-1-119-61738-9 (ebk)
ISBN: 978-1-119-61740-2 (ebk)

Manufactured in the United States of America

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2019943278

CONTENTS

INTRODUCTION

> “The most fundamental forces of cybersecurity are speed and connectivity. Our solutions must support and leverage these forces.”
>
> *Phil Quade,*
> *Fortinet*

> “Embracing cybersecurity as a science can be an incredibly powerful and effective way to underpin innovation.”
>
> *Phil Quade,*
> *Fortinet*

Humankind experiences some of its greatest disappointments and disasters when we fail to acknowledge the fundamentals of physics and chemistry. As we solve problems and improve technology, we must work with, not against, the foundation of the laws of mass, force, energy, and chemical reactions—laws that began with the cosmic big bang.

Like the physical world, cybersecurity has its own set of fundamentals: speed and connectivity. When organizations ignore these fundamentals, distracted by sophisticated marketing or new products, we suffer the consequences. We end up with solutions that solve only part of the problem or that simply stop working (or stop us from working when put to the test of real-world conditions).

That’s partly because, to date, cybersecurity has been treated as *a cost of doing business*, as opposed to *a foundational set of primitives and rules* that are leveraged to achieve greater things. To build a cybersecurity foundation that will work now and continue to work in a world exponentially faster and more connected, we must start treating cybersecurity more like a science. We must understand its fundamental elements and how they interact.

The early Internet, constructed decades ago to serve a small, tight-knit and primarily academic community, was built upon principles of game-changing speed and a deep understanding of the importance of connectivity. Security and privacy were not needed for that first small group of trusted users and thus were not part of the original design requirements. Although security and privacy have demonstrated their importance in today's blisteringly fast, global network, they have not kept up as the Internet has matured.

While we are exponentially more connected than at any other time in history, with nearly instantaneously accessible information at our fingertips, the cyberadversaries—not the defenders—are the ones who have mastered speed and connectivity to their advantage. Speed and connectivity serve us well as communication building blocks, but too often have failed us in cybersecurity, because we have failed to establish the foundation of cybersecurity upon those fundamental elements.

In a hypercompetitive business landscape, not only do cybersecurity fundamentals protect you and make you a much less attractive target to bad actors, but they also cast a halo of protection across all the individuals and organizations to which you are connected.

When we build our cybersecurity based on a complete understanding of fundamental elements and how they can work together, we can inspire and encourage scientific revolutions and evolutions in cybersecurity that will make us much better off.

We are on the verge of a new understanding of a basic element of human society. Just as the world has understood that economic security has been highly dependent on a stable flow of fossil fuels and that national security is dependent on safeguards for nuclear weapons, today we understand that, in our hyperconnected world, there is no global security without understanding and mastering the science of cybersecurity.

But the real historical analogy of cybersecurity, the story of the digital big bang, starts much earlier. Let's rewind nearly 14 billion years to the Big Bang, the beginning of the universe as we understand it today.

> "The good thing about science is that it is true whether you believe it or not. That's why it works."—*Neil deGrasse Tyson*

THE COSMIC BIG BANG: THE BIRTH OF THE PHYSICAL UNIVERSE AND THE HUMAN SOCIETY THAT EMERGED

At the beginning of time as we know it, around 14 billion years ago, energy and matter were born in a moment of unfathomable brilliance. Those core building blocks combined into atoms, followed by even more complex assemblies (molecules) just a few hundred thousand years later.

Billions of years later, after countless stars were born and died out, our solar system was formed from the remnants of furnaces of those long-dead stars. Physicists and chemists study the big bang's fundamental elements and their interactions in part to explain what things are made of and how they behave.

Some of those complex configurations coalesced into what we call *life*. We study life and how it evolved from its most primitive state to discover where we come from and to help us thrive within our given universe, not fighting mother nature.

The human life that eventually emerged from among this plethora of creatures eventually formed complex rules and societies that evolved in a broad set of stages or ages. Yuval Noah Harari in *Sapiens* cited them as follows:

- The Cognitive Revolution (c. 70,000 BCE, when Homo sapiens evolved imagination)
- The Agricultural Revolution (c. 10,000 BCE, the development of agriculture)

- The unification of humankind (the gradual consolidation of human political organizations toward one global empire)
- The Scientific Revolution (c. 1500 CE, the emergence of objective science)

In each of these ages, humans made relatively large leaps forward in understanding their environment and, at times, directly shaping it.

THE DIGITAL BIG BANG: THE BIRTH OF THE DIGITAL UNIVERSE

If we take on the mindset of a cybersecurity historian, we can look at the big picture in the same way and attempt to understand what is driving it forward. Consider these observations:

- While it took billions of years for the physical world we know to create and sustain human life, it took just 50 years from the beginnings of the Internet as ARPAnet in 1969, for the explosive forces of digital speed and connectivity to transform human society.
- Ninety percent of all the data in the world ever created was generated in the last two years. Bang!
- The Internet itself—a vast and hyperconnected data transmission system—now creates *2.5 quintillion* bits of data per day. I don't even have a fathomable analogy to characterize how much that is—but it's 18 zeros.

Digital technology has come to enmesh and propel nearly every aspect of modern life, from the operational infrastructure that keeps our cities and towns powered and functioning, to the now almost entirely digitally driven systems of global finance, security, and energy production. The rapid transference of digital information is how we connect, communicate, and—in many ways—sustain human life, order, and a tentative semblance of peace on Earth.

Our opportunity is to describe how the digital big bang progressed over time, understand its significance, and do something smart and productive about it.

THE SCIENTIFIC REVOLUTION

After the cosmic big bang, billions of years passed before humans came along and eventually started trying to make sense of the whole thing.

In human history, the most recent and most significant age is the Scientific Revolution, not so much because of what it achieved, but because of what it left behind. It was in the Scientific Revolution that we finally admitted that *we didn't know everything*. The admission of ignorance advanced the pursuit of knowledge and reason. It allowed us to define the modern laws of physics and chemistry; to explain, in a data-driven way, how nature's fundamental elements interact; and to discover the perils? of ignoring those laws. It incentivized us to fill in gaps in our data collection that we didn't feel obliged to before.

For example, the maps of the world from 750 years ago had elaborate drawings of mid-ocean whirlpools and sea monsters—here be dragons—mid-continent mountain ranges, and other physical phenomena. Faulty thinking, and the desire to warn of the dangers of sea exploration, led mapmakers to fill in what they did not know.

In contrast, the maps of the Scientific Age were drawn with large blank areas, showing where we had no data. It was not until we admitted that we in fact had very little idea what was beyond the horizon, or mid-ocean or continent, that we began exploring those areas and filling in the missing pieces that led to a much better understanding of our world.

The pull of curiosity about basic principles reduced the fear of the unknown and prompted the physical world's golden age of scientific education.

Now we must make the same leap in cybersecurity. We need to stop quaking at the cyber threats—real and imagined—and get down to the business of defining how to navigate and master those threats.

THE BANG BEGINS

A masterpiece of international collaboration, the Internet has its roots in the desire to share computing and information resources and the US Department of Defense's goal of establishing connectivity via computers in the event of a nuclear attack that destroyed telephone systems.

On October 29, 1969, the first message was sent over what would eventually become the Internet. Meant to be the word "login," the letters "L" and "O" were sent from researchers at UCLA to a team at Stanford. Then the system crashed. (We'll pause while you chuckle about that first crash.)

When it was constructed and deployed, the Internet served as a communication platform for a tightly restricted group of specific users.

With the advent of packet switching—the division of information into smaller blocks to be transmitted and then reassembled, pioneered as a Cold War strategy—that communication became a viable, though intensely limited, reality.

WHAT WE GOT RIGHT

Internet pioneers got speed and connectivity right—the digital big bang's equivalent of matter and energy. Their goal was a secure, distributed widespread computer communication system, and they achieved that goal.

WHAT WE GOT WRONG

Because the digital transmission of information was so restricted in both users and data, the use of ARPAnet was governed by a shared sense of trust that was informed and enforced by security clearances, professional accountability, and total lack of anonymity.

AN UNWARRANTED ASSUMPTION OF TRUST

With this assumption of trust, things went off-kilter. That assumption thwarted the parallel development of security, particularly trustworthy authentication, that could have supported the speed and connectivity that would make the Internet transformational.

With the passage in 1992 of the Scientific and Advanced-Technology Act, research and academic institutions started using this early Internet. Security shortfalls were generally understood, but the circle of institutions that had access remained small and tight-knit. It wasn't until 1993, and the release of the first web browser that Internet access became mainstream. At that point, both the Internet and its security, or lack of security, achieved greater significance.

The assumption of trust that was still deep within the DNA of the Internet became a huge problem the moment the public could go online. On an increasingly vast and anonymous network, that trust soon transformed from guiding philosophy to greatest weakness. As more people arrived, the Internet quickly became a newly discovered continent of naïve users, systems, and networks to be exploited and hacked for digital fraud, grift, or simply to prove it could be done.

Since those first hacks, the field of cybersecurity has struggled to catch up and compensate. Mitigating the weakness—the wrongful assumption of trust and the lack of strong authentication—while still balancing the essential benefits and fundamentals of speed and connectivity, remains an enduring challenge of cybersecurity today.

AN HONEST ASSESSMENT OF THE CURRENT STATE

For all the stunning power of its speed and the vastness of its data, the Internet is shockingly fragile and fallible. We're propping it up, sometimes with ridiculously complex schemas and other times with little more than digital Popsicle sticks and Elmer's glue and, for high-end applications, duct tape.

The Internet is fast, anonymous, powerful, and profitable—all factors that have accelerated its use and deployment—while at the same time prone to malicious exploitation, with terrible potential for criminality and sabotage. The continuing series of breaches of organizations of all levels of sophistication shows what a huge problem we have.

WHAT CYBERCRIMES EXPLOIT

Perhaps what is most amazing (or at least ironic) about cybercrime is how this masterpiece of technological collaboration and human connection is so often exploited to gratify human impulses. Distributed denial-of-service (DDoS) attacks, phishing emails, and

THE DIGITAL NUCLEUS

As mentioned earlier, the most fundamental forces of cybersecurity are speed and connectivity. Our solutions must be built to support and leverage these forces.

Although security has historically slowed things down, security without speed is a losing proposition. Similarly, security is only as strong as the weakest link in the chain, so security must enable connectivity—specifically, an integration of your defenses to leverage your strengths. This is a far better core strategy than the common alternative: expecting your weakest point to be better than the adversary's strongest methods. To achieve not only optimal but even basically functional cybersecurity, we must have speed, connectivity, and integrated cybersecurity.

In the pages that follow, we will explore the scientific forces of speed and connectivity that must shape our approach (see Figure 1). We must show how to harness and amplify these forces with cybersecurity that offers greater degrees of precision to counter the increasing sophistication of threat actors and cybercriminals.

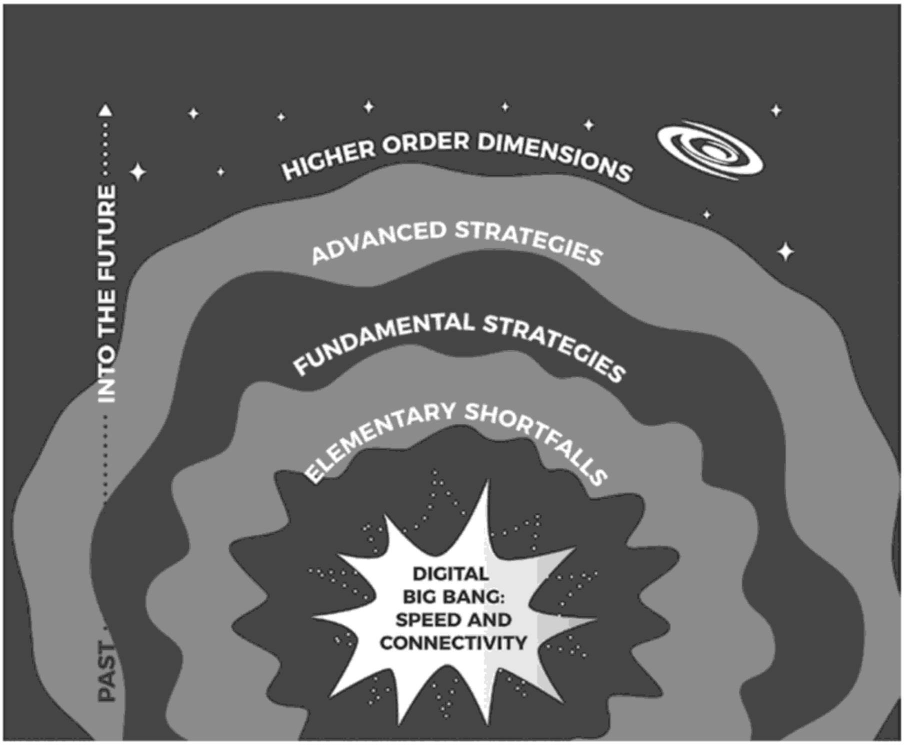

Figure 1 Speed and connectivity form the nucleus of the digital big bang.

We will explore how we can create a more scientific approach to cybersecurity, based on accurate assumptions. We will probe the essence of the modern problems we face and see how lessons from the world of science extend to cyberspace, leading us to certain inevitable mind-expanding conclusions about the very nature and order of how cybersecurity must evolve.

This book is divided into parts. Part I explores the digital nucleus of speed and connectivity.

Part II details the elementary shortfalls in the areas of authentication, patching, and training, and Part III discusses fundamental strategies of access control, cryptography, and segmentation.

Part IV covers advanced strategies, including visibility, inspection, and failure recovery, and Part V lays out higher-order dimensions we must account for, including complexity management, privacy, and human frailty.

In keeping with the spirit of the Internet's invention, this book is a collaborative effort. For each of the topics mentioned, we will hear from some of the leading experts in cybersecurity today, across industries and disciplines, as they come together to offer their insights.

We define success as enabling a pace of innovation in the field of security that outruns the inevitable attempts by adversaries to do their dirty deeds.

It is our hope that by focusing on the fundamental and foundational principles of the science of cybersecurity, this book will empower those who fight the battles to achieve more effective, efficient, and consistent victories for many years to come.

the **Digital Big Bang**

THE DRIVE TO CONNECT

The Internet's creation was a testament to the power of collaboration. Researchers realized that they could achieve more insightful results by comparing and combining their efforts and getting access to remote computing resources.

The resulting architecture was designed around rich and resilient connectivity. As it matured, the Internet fulfilled deep needs for speed and connectivity—organizational, financial, physical, mental, and even emotional—which catalyzed its unprecedented proliferation.

But that highly desired connectivity also opened the door to attacks. Attackers soon learned that they could use connectivity to their advantage to achieve a malicious effect without being near their actual target. Adversaries now can launch attacks from multiple places, focusing their multifaceted barrage on points of weakness. Perhaps it is the central dilemma of cybersecurity: if you can connect with everybody, you can be reached by anybody.

Defenders should take the same architectural approach: design security that leverages connectivity.

HARNESSING SPEED AND CONNECTIVITY

Just as the cosmic big bang's fundamental forces of energy and matter must be carefully managed to achieve intended results, so too must speed and connectivity in the digital universe. For example, a split atom can do one of these two things:

- Blast and heat whole cities—Generate cool air in the summer and heated air in the winter via clean electricity from nuclear power plants
- Heat and blast whole cities—Generate fire and concussion via a nuclear weapon

Cybersecurity implementations must be efficient enough to enable both the highest possible safe speed at all times and the maximum reach and scope of connectivity.

Trying to build cybersecurity solutions that do not maintain speed and connectivity will fail, like an engineer who tries to ignore the laws of physics and chemistry. Just as the communication infrastructure of the Internet is based on a connected fabric of fast communication mechanisms, the security fabric that underpins communications also must be based on an integrated security strategy. Because speed and connectivity are the two primary elements of the Internet, harnessing their strengths and managing their risks must be the primary elements of any effective security strategy.

1

SPEED

“Speed is at the nucleus of the cyberfrontier.”

Roland Cloutier,
ADP

“Greater connectivity, faster transmission and processing speeds, and machine algorithms result in faster and potentially more accurate decisions.”

Scott Charney,
Microsoft

Speed must be viewed and treated like the fundamental element it is. But by its very nature, security slows things down. When you’re in the security business, you’re fundamentally in the business of slowing people down, and that’s a horrible business to be in. Security must harness the power of speed to secure information while protecting against cyberattacks at the same rates.

Simply put, all cybersecurity must be extremely fast.

Security without speed is a losing proposition. In fact, slow security is often no security. Good security strategy must be based on leveraging speed, specifically

- Raw speed to detect and mitigate attacks in real time
- Processing capacity with more sensors, more data, and more insights to parse data more efficiently and find the smallest anomalies in system functionality

- Forward compatibility to create the headroom to implement future solutions that could involve even greater speed

Good security strategy must achieve these goals with as little impact as possible on the speed users have come to expect and demand. That's because in addition to the operational reason for speed, there is a practical reason: Users aren't willing to wait.

A consistent consequence results from that user impatience paired with cybersecurity techniques that don't feature speed as a fundamental component: Slow security solutions get shut off, either because they are too cumbersome or because they simply can't keep up. A security solution that lacks speed and thus is turned off provides zero benefit. Thus, slow cybersecurity techniques become greater impediments than benefits.

If organizations are forced to adopt tools that do not meet the needs and standards of fast data transfer, the odds are that not only will those organizations become less safe, but they will carry that lack of safety to every point of connectivity they share, endangering other organizations.

Acknowledging the inherent conflict between security and speed requires us to strategically design how, where, and when to slow things down, while maintaining and preserving as much velocity and efficiency as possible.

When it comes to cybersecurity, without speed, there is nothing. Users will, however, embrace a solution with speed as its key component.

SPEED: THE NUCLEUS OF THE CYBERFRONTIER

Roland Cloutier, ADP

Context is king when providing tangible models of reference to complex issues like cybersecurity. Even as security practitioners, we are faced with an onslaught of information, intelligence, data points, and other exceptional information with a need for action or decision, but we often lack the availability of context to make sense of the environmental settings that help us make great decisions.

WHAT DO WE MEAN BY SPEED?

As we begin to discuss speed as a binding strategy and guiding principle for approaching cybersecurity, we must take the time to truly understand the implications and context of the meaning of speed as a multifaceted component of the threat, of what we are protecting, of how we protect, and of the impact on our ability to be successful.

Speed is in fact at the nucleus of the cyberfrontier. As a term, it can be considered a noun (the rate at which something is measured for movement) or a verb (describing an action of movement). In either case, when linked to the defense of technology, it is speed that dictates our plans, actions, and, often, outcomes. It is speed that supports measures of priority along with residual risk measures. And it is speed that impacts basic program considerations such as cost, services, and urgency.

We'll now explore key areas of speed as a binding strategy and the key strategic elements that you can focus on to help you make better decisions, deliver better results, and have a greater impact in protecting your charge.

HOW SPEED IMPACTS SECURITY

Living in a digitally connected ecosystem of business, societies, and global economies that operate at the speed of light means that the factors and issues that determine how and what we protect are intellectual property loss ruin your business? Can your business ecosystem outside your control cause irreparable damage? These questions and many others should be the foundational elements of how you describe your "business of security" and what your mission focus is. In turn, as you begin to consider the implication of the speed used against you and the speed that will help you accelerate your effectiveness, a deep understanding of your mission imperatives in alignment with the following five critical areas of planning will ensure your success in the hyperconnected and hyperspeed world in which you operate:

1. Understand your environment. Your success depends on your direct ability to succeed within the environment in which you operate. To do that, you need to understand your environment through transparency, knowledge, and access. This includes crucial elements such as understanding your critical assets, a holistic understanding of the resources and technology deployed through a comprehensive configuration management database (CMDB), and data flow diagrams that detail how information flows through your business. Just as important is the understanding of your third-party ecosystem, your supply chain, and how your services are in effect an integrated component of your customers' supply chains. Your ability to quickly understand the impact of any given event through this level of transparency is a fundamental component to being able to think and act quickly.

2. Drive safely at high speed. Your business success depends on speed to market and speed to respond. Your job is to get everyone there safely. This sense of speed enablement, or acting like the brakes on the car so your business is confident to go faster, requires a mature risk process. Effective risk programs have tiers of risk considerations and actions that create broad bands of flexibility and enable decision making based on preselected and informed risk formulas that serve as guiding principles. Spending time developing those mechanisms and allowing them to mature, educating your business, and just as importantly, educating your team will empower and enable all levels of the organization to recognize and facilitate business-based risk decision making at speed.

3. Plan ahead. Your opposition is well funded, utilizing capabilities and decisioning guiderails that are faster than yours. As in an old-fashioned gunfight, the first one to put lead on the target wins. This means that you need to be comfortable with rapid decision making based on accumulated knowledge rather than absolutes and have a "gun belt" of premade decisions, actions, and plans on your side. For instance, if you have a ransomware incident that is less than *x*% contained, do you shut down your data center? If you are suffering a financial crimes attack, will you call law enforcement, and if so, what agency and what is their number? Simple efforts such as tabletop exercises or defining preplanned partners significantly add to your ability to react fast in times of crisis. Prepositioned decision making agreed to by your leadership also ensures that your business will understand, support, and expect clear action and leadership from you when needed.

4. See the big picture. You need over-the-horizon threat modeling. I think everyone would agree that seeing a speeding train coming at you is better than getting run over by one. Unfortunately, too many people concentrate too myopically on their own operating environment and never look up long enough to see the train coming down the tracks. The use of intelligence services, information-sharing partnerships, and other mechanisms that give you a view outside your business into adjacent industries, like competitors or aligned ecosystems, are great ways to measure and prepare for the potential impact of issues not yet affecting your business. This greatly enhances your time to prepare, plan, and react to situations and opportunities that too often are missed because of insular behaviors.

5. Make the most of limited resources. Managing a business with limited return on investment (ROI), no profit, and smaller teams takes a different approach. Not every industry has the mission criticality of a nuclear power plant or the financial resources of the financial sector, and most of us never will. But just because we can't build large operating teams doesn't mean there aren't methodologies we can put forth to make us more nimble and adaptable. For instance, sometimes less is more. Often, many of the services we use are not employed on a constant basis, and