BECOMING A CYBER-AWARE CEO

PART ONE: THE BACKSTORY

Abstract

This two-part article will provide CEOs with an understanding of the challenges of the typical enterprise CISO and propose a new approach to satisfying mutual goals.

Part One: The Backstory focuses on how we got here. Written for a non-technical audience, the evolution of cyber is described to give CEOs the foundation of a practical dialogue between the business and the security teams. Like a marriage, where both persons unify in the same mission, but one person speaks from the heart and the other from the mind; the business and I.T. need a communication tool to bridge the communication gap.

A history of the world wide web

In 1983, US military intelligence invented a robust new method to communicate, in lightning speed, anywhere in the world. The "lab coats" called it TCP/IP, but five years later, scientists at CERN would build off this technology to create the World Wide Web.

For the first time in human history, the mass distribution of information was possible at a fraction of the cost of previous methods of communication and the world burst online in an attempt to capture the mindshare of customers, the industry, friends, and enemies.

Three decades later, we now find critical systems online supplying our electricity, medical needs, shopping, and whatever any smart would-be inventor decides in this new digital economy.

Obsession with the User Experience

Technology is inherently complex, hence Silicon Valley's obsession with the User Experience. Solving the problem of how people engage the intricacies of getting information online, the "App" economy is now a $3.3 trillion industry. This evolution has made it easy for any corporate employee to independently revolutionize how they achieve their business goals. As Steve Jobs famously exclaimed, "There's an app for that!"

Compare, for example, how I collaborate on important documents with my colleagues today vs. ten years ago. Dropbox and numerous other file-sharing apps now dominate this information-sharing process, making these third-party organizations the custodians of your private information. The less reputable of these apps attempt to lay claim to the intellectual property that's uploaded into their system. Why do you think it's free? They monetize your data and expressing surprise or aggravation is much like the cow complaining how the steak gets served!

Immediately after those original keystrokes from CERN, scientists had the foresight to know that information sharing would quickly evolve to include private communication, personal files, financial transactions, digital or physical assets, and intellectual property. And of these need to be kept private and secure.

Inventors around the world got to work. A few exemplary engineers founded what is now a well-established cyber security industry.

> "I was in a small country, I was in Israel," he says. "We felt isolated from the rest of the world. The internet looked like a huge revolution. But the question was what about security—how do we keep everyone outside our network? And so we matched a good idea in tech with the most revolutionary of markets and demand. We started Check Point."[1]
>
> – Gil Shwed, CEO and Founder, Check Point Software

Israel emerges as cybertech's start-up capital of the world

Over 25 years ago, a man named Gil Shwed invented, in "lab-coat terms," Stateful Packet Inspection. This became known as the Firewall. Meanwhile, in the United States, Anti-Virus was being created. At this point in IT security history, one would protect entire networks (many computers) with firewalls and the other individual computers with anti-virus.

1 "This Israeli Cyber Billionaire Battles Hackers In China, Russia And Iran: 'It Will Only Get Worse'," by Zak Doffman, Forbes, February 18, 2020

Since then, the cyber security industry has ballooned into a $114 billion per year industry, with almost 1,000 companies all competing for enterprise budgets, all with thousands of web pages for enterprises to sift through in order to find the cyber protections they need.

Stitching various solutions together vs. one governing seamless solution

Dating as far back as 5,000 years ago in China and Egypt, patching pieces of fabric together to create quilts kept people warm at night. The technology to create a larger, seamless piece of fabric wouldn't be invented until the spinning wheel, in the Indian subcontinent, in 1AD.

Today, patch working is mostly a tradition, but given the choice, I'd rather sleep under a full-length duvet. If we were to see someone on the street walking in patchwork clothing, we might think he or she is in desperate need for a new wardrobe or possibly auditioning for clown school!

Prior to the invention of new technology, humans "stitched together" whatever we could to satisfy our needs; small pieces of cloth, to make clothing and blankets. It still works today, but there's a better way.

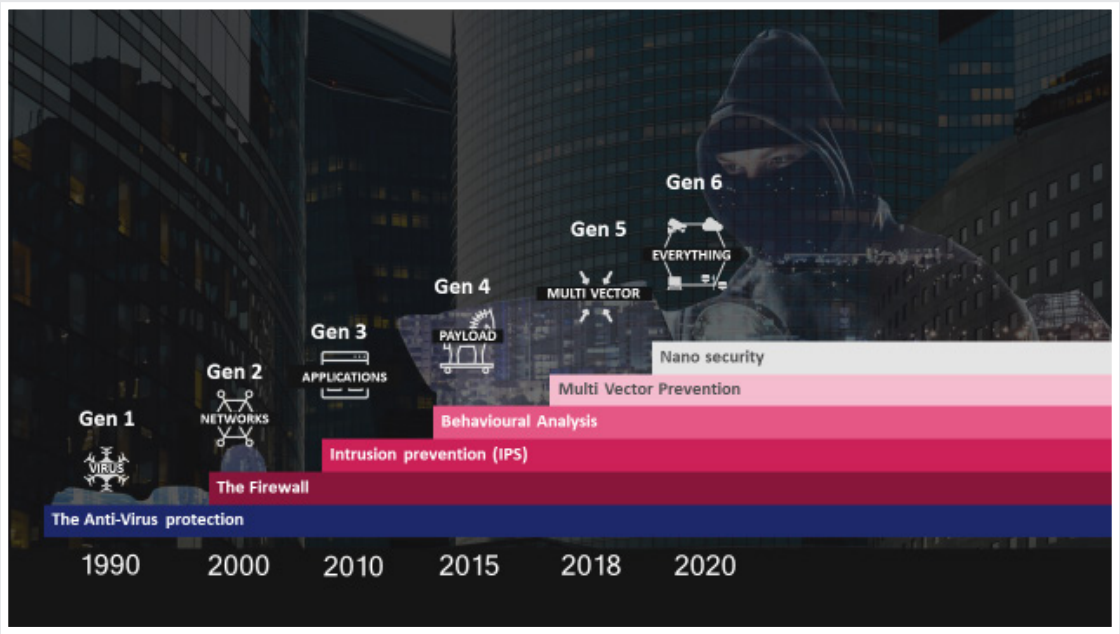
We've experienced a similar problem in cyber security. The organic, but rapid growth of enterprise online activity, has forced companies to stitch together cyber products in response to not only how the company has grown online, but also how cyberattacks have evolved and therefore require new technologies to counteract them.

Viewing the six generations of cyber security

We can summarize the past quarter of a century of cyber evolution through a generational lineage of attacks. The image below depicts the linear relationship between an advancing computing infrastructure and the security innovations required to resolve cyberattacks.

As mentioned earlier, at the birth of this industry in the late 1980s to early1990s, anti-virus (AV) was needed to keep individual computers safe. We'll call this Generation 1 attacks. Click here for a more technical example of a Gen 1 cyberattack.

Generation 2 attacks quickly followed in the 1990s, as cyber hacks started to spread from one computer to another, throughout entire company networks. This had a paralyzing effect on organizations, driving the creation of the firewall. So now, in addition to AV, companies added firewalls to their data centers; not just one, but to safeguard against equipment failure, they bought two of everything for each office location. Click here for a more technical example of a Gen 2 cyberattack.



In the late 2000s, Gen3 attacks required protection against threat actors gaining access to all those third-party applications your company uses to process critical information. This gave rise to intrusion prevention system (IPS) products. By adding multiple IPS technologies, we're beginning to see the "stitching together" of multiple cyber protection products found in all organizations. Click here for a more technical example of a Gen 3 cyberattack.

Generation 4 – Around 2015, we saw the rise of targeted, unknown, evasive, polymorphic attacks.That's a mouthful, but in essence, hackers have begun to use Machine Learning in cyber-attacks. These big payload attacks drove the increase in anti-bot and sandboxing products to add to the already-very-crowded collection of AV, FW and IPS technologies. Click here for a more technical example of a Gen 4 cyberattack.

Large-scale, multi-vector mega attacks shocked private and public organizations around the globe in 2018 when a new generation of attacks engaged entire countries in cyberwarfare. Russia allegedly attacked the Ukraine and caused massive devastation to their economy; but the cyber weapon couldn't be confined and the effects on enterprise corporations like Maersk, Mondelez and Merck (who had the money, methods and means to prevent such a catastrophic failure) resulted in billions of dollars of losses.

Gen5 protections and the advanced threat prevention technologies needed to keep countries and companies safe, are now stitched together with all the other choices from a maturing market of many cyber security vendors. Click here for a more technical example of a Gen V cyberattack.

> " With more and more devices connected to the internet every day, from self-driving vehicles to children's toys, it's safe to say that IoT devices are everywhere. Considering this, it should come as no surprise that vulnerabilities found in IoT devices have more than doubled since 2013."[2]

This brings us up-to-date with the current Generation 6 of cyberattacks! The rapid technological advances over the past few decades and the invasion of increasingly more sophisticated hackers, cybercriminals, and nation-state threat actors, has forced the cyber security industry to produce more and more products. This meant that vendors now have to replicate their solutions for personal computers, tablets, smartphones, computer servers, the Cloud (which is to say, someone else's computer) and the Internet of Things (IoT). It is estimated by CSO Online that the average corporation uses approximately 70 different cyber vendors, all with multiple-devices, across multiple locations, with thousands of connections and therefore vulnerabilities. Click here for a more technical example of a Gen VI cyberattack.

Additionally, the IoT marketplace is estimated to stretch from 6 billion devices today, to over 20 billion in only five years. The problem this causes for your security teams is the unknown; that anyone in the corporation can introduce an unlimited number of IoT devices into the offices. Plus, how does a CISO secure a smart-thermostat? Companies need security products attached to all these devices!

2 "IoT security failures are not child's play," by Chetan Conikee, ITProPortal, April 8, 2020

Complexity is the enemy of security

As organizations have grown their online operations, they've opted to select security products considered best of breed for each type of attack. Today, most organizations maintain a closetful of disparate technologies that are optimized within the confines of individual vendors. They lack integration with products from other vendors, and resolving this situation has become the burden of the customer. Plus, they must find the personnel to operate multiple products, impacting PandL statements.

Complexity is the enemy of security. *If security isn't simple, it isn't followed*. A perfect example is the requirement of alpha-numeric passwords, with symbols, UPPER CASE, lower case and at least eight digits. Can you easily remember X4sd!b#0? No, so people write their passwords down, thus reducing security, when studies have shown that passphrases are easy to remember and more secure. In fact, NIST's latest guidelines no longer recommend that end users change their passwords every few months, because people tend to run out of complex things to remember and then resort to one password everywhere or they think they're outwitting hackers with small logical changes to help them remember.

It's time to share the burden of complexity.

Cyber sox

In 1997, WorldCom and MCI announced their US$37 billion merger, making it the largest corporate merger in U.S. history at the time. World dominance was the next step for MCI WorldCom, but disaster struck when it was suddenly discovered that the Directors had used "accounting irregularities" to push up the stock price. As a result, 30,000 people lost their jobs (and health plans and 401Ks), investors lost $180 billion, and the CEO received a 25-year jail sentence.[3]

The Sarbanes Oxley Act of 2002 (SOX) now requires the CEO and CFO of publically traded companies to issue a statement certifying that "financial transactions and disclosures fairly represent, in all material respects, the operations and financial condition of their company;" enforced by the SEC and subject to a prison term of up to 20 years.

Like all new initiatives, SOX was slow to be adopted, but when the SEC filed charges against more CEOs, business leaders began to pay attention and today, CEOs receive a weekly SOX report from their CFOs, in an effort to safeguard against fraudulent practices.

"Today's CEOs need a weekly cyber briefing, but not about technology, about risk" says Peter Alexander, the Chief Marketing Officer of Cyber Security firm, Check Point Software Technologies.

3 "The 10 Worst Corporate Scandals of All Time," Accounting Degree Review

Conclusion of part one

The least we speak the same language, the more energy we must exert to try and understand one another, rather than resolving our actual challenges. While listening is important, those gifted with technical athleticism are engaged in the heat of battle every day, so time is of the essence.

Part Two of this paper provides a framework for a cyber briefing that CEOs can use when expecting highly technical team members to engage with the business, and with communication in business terms.

We've provided an interactive plug-and-play matrix to bridge communication gaps and provide the expedience your cyber teams need to act on critical threats. This is combined with the satisfaction from the business leaders that budgets are correct, assets are protected, and the reputation of the business is held in high esteem.

For additional executive-level security insights, go to cybertalk.org.

Edwin Doyle is a Global Security Strategist for Check Point Research, the academic branch of Check Point Software, a leading provider of cyber security solutions. For over 20 years, Edwin has communicated with international leaders in security, cyber forensics and cyber law enforcement. He frequently shares cyber defense best practices with media, government agencies, and enterprise organizations.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com