Cybersecurity as a competitive advantage is the next big strategic play

Tamara Schwartz,[1] Jose Ignacio Parada,[2] Fred Cohn,[3] George Wrenn,[4] and Keri E. Pearlson[5]

[1] York College of Pennsylvania, York, PA

[2] Sloan School of Management-Massachusetts Institute of Technology, Cambridge, MA

[3] Schneider Electric, Boston, MA

[4] Bain & Company, Boston, MA

[5] Sloan School of Management-Massachusetts Institute of Technology, Cambridge, MA

[1] tschwartz@ycp.edu, corresponding author

Abstract

In a world of increased cyberthreats, cybersecurity is still viewed as a necessary infrastructure cost delegated to the IT team. This research seeks to disrupt that paradigm by exploring how cybersecurity can create a strategic advantage. Theory building case study is combined with a theoretical synthesis of Porter's Five Forces and Cusumano's six principles of staying power to propose four strategies to achieve a competitive advantage with cybersecurity for those leaders brave enough to embrace the opportunity.

Changing the Value Proposition for Cybersecurity

A cybersecurity investment changed the heating, ventilation, and air conditioning (HVAC) industry when a company in the industrial equipment sector developed a HVAC system with built-in cybersecurity. The investment was made for information security, but achieved an unexpected outcome: it changed customer expectations of HVAC systems and restructured the HVAC industry. The product was built on a secure, cloud-based platform and supported security updates – unprecedented features at the time. By including built-in cybersecurity, the product differentiated itself and reduced the threat of new entrants, making it less of a commodity and thus, harder to be substituted. What began as an infrastructure investment became both a core capability and a product differentiator, all of which created a competitive advantage!

Cybersecurity leaders understand their role is to facilitate the management of cyber risk, but too many C-suites see cybersecurity as a necessary expense or worse, an impediment to action. The focus is on protecting the firm, and the CISO is expected to prevent security breaches. Thus, cyber risk is dismissed as a non-integral part of strategy. Although leaders identify strategic business priorities, cybersecurity rarely makes the list. Instead, it is delegated to Information Technology (IT) operations as an infrastructure investment (Hepfer and Powell, 2020). In fact, prior to 2014, the term cybersecurity "was rarely heard of or directly addressed at the board level" (Islam and Stafford, 2017). But things are beginning to change. Following the Covid-19 pandemic, 88% of boardrooms now regard cybersecurity as a business risk rather than just an IT problem. Good news for cybersecurity executives, but the problem remains – how do we frame the cybersecurity value proposition? When executives focus only on risk, they miss the business opportunities.

Digital Transformation: Past as Prologue

When the information revolution swept through the economy in the 1980s, the reduced cost of obtaining, processing, storing, and transmitting data was so dramatic that few managers disputed the value of capital investments in IT (Porter and Millar, 1985). Over time, these investments transformed from infrastructure expenses to strategic business opportunities – digital transformation had a clear value proposition. The infrastructure investment increased data access and supported stronger core capabilities and business processes. It also became a new product or a differentiator in existing products. It created advantage!

Digitalization also made strategy and value creation fiercely dependent on IT, so the frequency, magnitude, and impact of cyberattacks are capturing board attention (Islam and Stafford, 2017). Cybersecurity investments have the potential to change from an infrastructure expense to a business opportunity with similar effects. C-suites understand cybersecurity is necessary for competitive parity – that its absence creates a strategic disadvantage. We argue that cybersecurity done well not only adds value, but is also rare, inimitable, and when highly organized, can create a sustained competitive advantage (Newbert, 2008).

When Porter (1979) introduced the Five Forces Model, he observed that "Many managers concentrate so single-mindedly on their direct antagonists in the fight for market share, that they fail to realize that they are also competing with their customers and their suppliers for bargaining power" (p.145). The digital transformation gave access to criminals, nation states, and other hackers, allowing them to compete with commercial and financial organizations to gain a competitive advantage through data theft, or by denying or disrupting access to key information systems (Schwartz, et al., 2019), but hyperattention to known competitors – market rivals, customers, and suppliers – reduces attention to these new cyber competitors.

Although these new rivals do not compete for traditional market share, their access can disrupt or deny access to core capabilities. It can give traditional rivals access to proprietary data or damage brand image. Inattention to these cyber rivals results because they are not in direct market competition with the firm (Schwartz et al., 2019). To paraphrase Porter (1979), "Many managers concentrate so single-mindedly on their direct antagonists in the fight for market share" (p. 145), and the competition "with their customers and their suppliers for bargaining power" (p. 145), that "they fail to realize that they are also competing with" (p. 145) hackers intent on disrupting their operations and stealing their data.

The company who thwarts these new rivals does more than maintain parity with traditional market competitors, they create a competitive advantage. Because digitization tied IT infrastructure to protection and governance of customer data, a strong cybersecurity culture, coupled with dynamic capabilities, enables organizations to operate through and recover quickly from an attack, creating a cost advantage. As part of infrastructure, it supports operations, while becoming a differentiator in platform business models. Last, a cybersecurity culture can lead to the addition of cybersecurity features to differentiate commercial offerings.

Cybersecurity at MIT Sloan leads an Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)3. The membership includes senior executives from 23 critical infrastructure companies. We conducted a series of surveys and semi-structured group interviews with these CIOs, CISOs and other senior executive industry experts, asking questions like: "What if we could change the cybersecurity conversation? Can cybersecurity features improve competitive position and capture market share? Do you know of a case where cybersecurity created an advantage?"

Numerous interview participants expressed frustration that many executives still perceive cyberattacks to be random, missing the fact that attacks can be intentionally designed to exploit weaknesses in firm strategies and capabilities, and missing opportunities. Leaders see cybersecurity as a sunk cost. We propose that if cybersecurity were to be viewed as a business opportunity, that it will create a competitive advantage. Instead of a sunk cost, it would be considered a strategic prospect with a Return on Investment.

Since boards and C-suite leaders understand how to have conversations about business opportunities, this paradigm shift would open the conversation about investing in cybersecurity to executives engaged in operations, marketing, sales, and strategic planning. Our aim with this paper is to facilitate a dialog about cybersecurity that includes everyone in the C-suite. Developing a business case for cybersecurity will add value and drive investment in physical and cybersecurity for your organization. This makes recasting cybersecurity as a competitive advantage a challenge organizations must master.

Change Behavior to Achieve Different Outcomes

Too often organizations perceive the cost of cybersecurity as the price of a new server, the salary of a new employee, the cost to recover from a breach or price of network analysis tools. Many companies persist with outdated software, failing to apply necessary patches for compatibility reasons. For example, operating unpatched Windows 2000 servers because they would not invest in new servers was one factor at play during the NotPetya attack that crippled Maersk in 2017 (Greenberg, 2018). Instead of asking how much new security measures will cost, organizations might consider the value to the business of cybersecurity resources spent on people, processes, and technology or how an investment in security might create a competitive advantage. Changing the question changes the conversation.

We asked interviewees, "If we could change the conversation from cybersecurity as an infrastructure investment to a strategic investment, what would that look like?" The CISO of a large network telecom company described cybersecurity as "table stakes," declaring "a lack of cybersecurity in 2022 is a competitive disadvantage." Others in the discussion considered the question and suggested that they had observed several situations where cybersecurity was considered a business opportunity driven by customer demand. Simply put, it was a reactive behavior, instead of a proactive, strategic intention. For example, we learned from an interviewee in the financial sector, that their customers increasingly demand cybersecurity, prompting the company's executives to ask, "Instead of just reacting to satisfy clients' demands, how can this need be transformed into a competitive advantage and integrated into the corporate strategy?"

Research Methodology

Using a theory-building case study approach, we looked for examples of competitive advantage tied to cybersecurity investment. A non-random sampling approach is typical in case study research because there is no representative sample of a larger population. By its nature, a strategic competitive advantage is difficult to replicate, making case study methods a valuable tool in strategy research because they focus on the dynamics of phenomena in specific environmental contexts (Ridder et al., 2014).

In addition to cases identified through the surveys and interviews, additional cases were identified using both Lexis-Nexis and Google to find articles in the popular press and in practitioner and academic journals. We cross-checked what we learned by studying corporate websites to examine cybersecurity services, practices and products that were highlighted by the surveys, interviews and journal articles. This resulted in a dataset of thirteen case studies across a variety of industries.

Mainstream research plays a critical role in case study analysis to support pattern matching (Dillon & Taylor, 2015). We used a pattern matching technique to compare empirical patterns within the case studies with the patterns of strategic advantage as understood in Porter's Five Forces and Cusumano's Six Principles of Staying Power. To expand theoretical constructs of competitive advantage, we conducted cross-case analyses to compare non-cybersecurity case examples conforming to the strategic advantage principles, with cybersecurity case examples where cybersecurity was specifically leveraged to create differentiation and staying power. Finally, we developed a new model by synthesizing the Porter and Cusumano frameworks based on the empirical patterns we found within the case studies.

Cybersecurity Model for Competitive Advantage

The pursuit of competitive advantage is a "holy grail quest" for strategists. The speed of change makes sustained competitive advantage ever more elusive as executives must demonstrate the ability to respond to disruption (Baran and Woznyj, 2021). And yet, in the quest to achieve competitive advantage, executives often fail to recognize environmental change, instead benchmarking existing market leaders to successfully build yesterday's competitive advantages (Christensen, 2001). Competitive advantage can be rooted in business models, processes, core competencies, or market positions. In the digitally transformed business, every one of these sources has an information component. The right information at the right time is the essence of competitive advantage (Porter and Millar, 1985). The value of information drove digital transformation, and that demands the strategic application of cybersecurity.

Porter and Millar (1985) anticipated that the trend toward information intensity would transform the economy and change the nature of competition as industries moved toward higher information content in both product and process. This prompted them to ask, "How will advances in IT affect competition and the sources of competitive advantage? What strategies should a company pursue to exploit the technology? Of the many opportunities for investment in IT, which are the most urgent?" (Porter and Millar, 1985). They saw three possible outcomes when IT was harnessed to create competitive advantage: a change in industry structure and the rules of competition, new ways to outperform rivals; and the spawning of new businesses.

As executives began to see their rivals leverage information for competitive advantage, they recognized the need for direct management involvement in the implementation of new technologies to realize Porter and Millar's (1985) predicted outcomes. In *Staying Power: Six Enduring Principles for Management Strategy and Innovation in an Uncertain World*, Cusumano (2010) proposes six principles for responding to the rapid change of technological disruption in an economy transformed by the information revolution.

Cusumano (2010) proposes platform and service-based strategies that rely on an IT ecosystem to generate innovative offerings as differentiators in the marketplace. He further suggests that firms go beyond strategy to build distinctive organizational capabilities that can expand scope and create a strong foundation for innovation and agility to respond to market demands. The strategic employment of technology to achieve these ends has the potential for tremendous cost savings as well as firm differentiation in the marketplace.

Cusumano's (2010) six principles, with IT as the foundation, led us to ask new interview and survey questions with respect to cybersecurity, such as "How have advances in IT expanded the competitive environment? How are new cyberspace rivals exploiting technology investments to deny access to the sources of competitive advantage and disrupt operations? What are the implications of cybersecurity investments that competitors might have made? Of the many necessary or potentially strategic investments in cybersecurity, which are the most urgent and which might create the greatest opportunity?"

Interview participants expressed strong interest in research that could demonstrate how cybersecurity can create competitive advantage. One study participant identified an instance where their employment of a particular cybersecurity software had enabled them to win deals over their competitors and develop clients because he had figured out how to sell cybersecurity as a competitive advantage, but he expressed concern that "advertising your cybersecurity could put a target on your back." Our interviews confirmed that organizations understand an absence of cybersecurity creates a competitive disadvantage, but that they are still struggling to articulate the value proposition for cybersecurity as a differentiator or cost eliminator.

The analysis of our case studies led us to synthesize the Porter and Cusumano frameworks, resulting in four specific strategies that can turn cybersecurity into a competitive advantage: 1) stratify cybersecurity across commercial offerings, 2) embed cybersecurity across the scope of the organization, 3) develop enterprise-wide dynamic cyber capabilities, 4) build organizational agility with cybersecurity. In some instances, organizations were experimenting with just one of these strategies, but we discovered that when they are employed together, they reinforce one another to create considerable staying power.

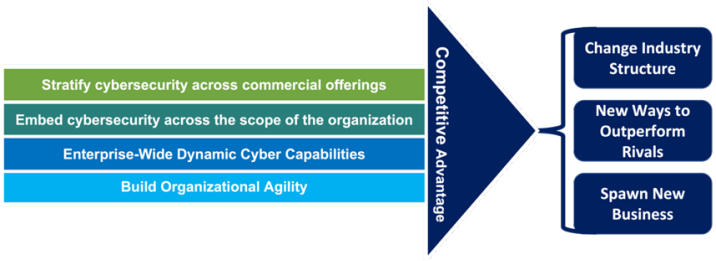

Figure 1: Condensed Structuring Cybersecurity for Competitive Advantage

Strategy 1: Stratify Cybersecurity Across Commercial Offerings

Cusumano (2010) recommends that companies can build a competitive advantage by focusing not just on products, but also platforms. He further suggests that product and platform offerings be extended with services. Because networked systems can be vulnerable through any element of the larger ecosystem, these first two principles need to be combined to realize the power of a competitive advantage.

Figure 2: Stratifying cybersecurity from products to platforms to services

Cyber Reliant, which offers data management services, added a data protection product through a collaboration with Lloyd's of London. By adding a cybersecurity insurance product, Cyber Reliant was able to add a warranty to their platform based data management services. Specifically, they employ anti-ransomware data protection technology to provide a warranty up to $5 million to their customers. By

stratifying cybersecurity across their commercial offerings of product, platform and services, Cyber Reliant added an insurance product to differentiate itself and create a new way to outperform their competitors.

Strategy 2: Embed cybersecurity across the scope of the organization

Scope efficiencies can be readily applied to cybersecurity by treating it as a core competency across the organization, not just as an infrastructure need. Building a culture that embraces cybersecurity can position a firm to create enduring competitive advantage. For example, a contemporary cybersecurity practice known as "shift-left" involves building cybersecurity capabilities as early as possible in the software development lifecycle. Typically employed by modern software firms, shift-left solidifies cybersecurity as a core product capability that percolates through all aspects of the product (Pearlson and Huang, 2022).

Because cybersecurity becomes a cultural mindset, it not only impacts firm R&D, but it can allow marketing and product development teams to leverage cybersecurity and respond to market signals regarding privacy. This enables them to pull new ideas from the customer base and intentionally embed cybersecurity up front. Shift-left is considered a superior practice to simply adding on cybersecurity at the end of the development lifecycle, when it becomes much more costly (Christensen, 2001). As cybersecurity becomes embedded across the scope of an organization, it drives financial benefits similar to economies of scale.

Figure 3: Include cybersecurity across the entire organizational scope

During the pandemic, with employees working from home, organizations demanded stronger security from the firms that enabled remote work. Slack enhanced security by giving firms more data visibility and control (Slack, 2020). This decision was both an infrastructure investment and a product enhancement. The nature of cybersecurity made it both. Improving security for clients required Slack to improve their own security. With cybersecurity built into the platform, it directly impacted their platform-as-a-service business model.

Strategy 3: Develop enterprise-wide dynamic cyber capabilities

Its widely accepted that firms should first develop core capabilities and then look to build strategies that rest on those capabilities (Newbert, 2008). Core capabilities create advantage because they are not easily replicated, giving a firm the ability to outperform their competitors. When a competitor attempts to replicate a firm's strategy, it is unlikely to succeed if that strategy relies on a differentiated core capability or knowledge base. This inimitability enables a long-term strategy and creates a high barrier to entry.

In order to engage competitors in the persistently unpredictable environment of cyberspace, firms require an adaptive, strategic cyber capability that can allow them to respond to rapid change. For example, following a security breach at WhatsApp, Signal, a competing messaging app in India, embedded cybersecurity into its platform and made secure messaging their core capability. With secure messaging as a core capability, Signal outperformed WhatsApp, even when WhatsApp attempted to introduce secure messaging. Customers migrated to Signal, because cybersecurity, and by extension, *privacy*, was the foundation of their business strategy (Chaturvedi, 2021).

Strategy 4: Build organizational agility with cybersecurity

Flexibility in cybersecurity is crucial. There is constant change in threat vectors, an increasing variety and number of bad actors, and new security vulnerabilities cropping up daily. Firms with the flexibility to constantly adapt to the evolving landscape will find themselves with an enduring competitive advantage, while less flexible organizations fall behind and fail to respond at speed.

When cybersecurity becomes a core capability by implementing the above practices, organizations can become extremely agile. Adaptive cyber capability integrates automation, defense, and enhanced decision making across the full scope of the organization (Schwartz et al., 2019). This adaptive cybersecurity behavior can enable a firm to pivot quickly in the event of sudden events such as changing market demand, black swan events, or new opportunities. When a firm can operate through and recover quickly from cyberattacks, while capitalizing on new market opportunities, it can generate considerable staying power.

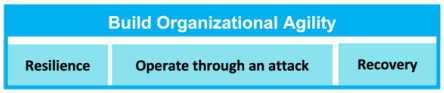

Figure 4: Cybersecurity increases agility

For non-cybersecurity companies, investing in secure infrastructure can allow quick adaptation to market changes. The Covid-19 pandemic forced companies to pivot quickly. Thanks to its investment in cybersecurity, Zoom was able to swiftly adapt and improve their security posture. Their rapid response to customer demands for secure video conferencing, not only improved their capability, but captured nearly 50% of the market share in the United States and United Kingdom in just under a year (Brandl, 2022).

The individual examples of applying each of these four strategies indicate applying just one can create a competitive advantage. However, our evidence suggests that when cybersecurity is applied strategically across the entire operation, that powerful synergies among these four strategies are a force multiplier.

Employing all four strategies in harmony leads to significant reshaping of industries, creation of new business opportunities and the ability to outperform competitors through cost reduction or differentiation. The following cases demonstrate these strategies in action.

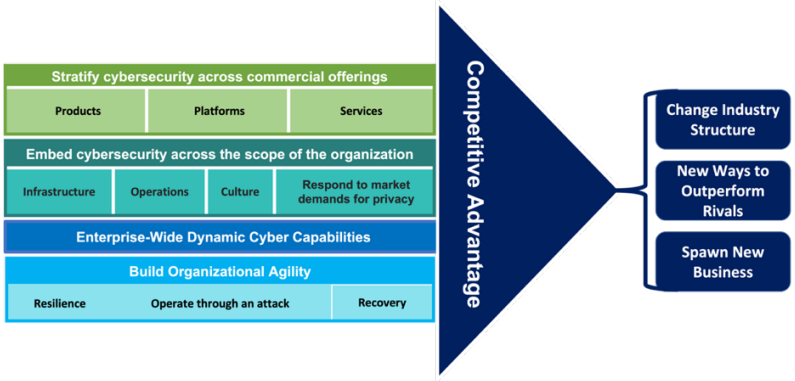

Figure 5: Full Model of Structuring Cybersecurity for Competitive Advantage

Creating Competitive Advantage with Cybersecurity

Case Study #1 Critical infrastructure company

One provider of critical infrastructure systems from our focus group learned that their customers were struggling to properly assess cybersecurity risks, train their teams to understand and manage cybersecurity products, and deploy cybersecurity protection, detection and response systems in this unique environment. While the customer's IT department was skilled at protecting the HR, Finance, ERP, Servers and Endpoints of the enterprise, the Operations Technology (OT) environment was foreign to them. Specific equipment and the necessary skills to properly secure the environment were unavailable within their teams. The supplier saw the opportunity and was able to upskill its own organization's service and support teams with specific cybersecurity expertise to provide those services in a consultative sales model. It found that this upskilling and alignment with its sales channel allowed it to add this service to its offer portfolio, increasing revenue and increasing the level of engagement and intimacy with the client.

Table 1: Critical infrastructure Company's Cybersecurity Strategy for Differentiation

Strategy	Cybersecurity Strategy	Sample Offerings	Competitive Outcomes
Stratify Cybersecurity across commercial offerings	• Deploy cybersecurity technology in company's own operational technology (OT) environment. Then leverage that knowledge to provide products and services to customers of similar need	• Vulnerability scanning • Network anomaly detection • Enterprise-grade Firewall	• Spawn New Business

Embed cybersecurity across the scope of the organization	• Take cybersecurity technology and knowledge and transfer skills from IT systems management to R&D, Operations, and Customer Delivery organizations	• Externally certified products and processes • Digital Offers that collect, store, and protect client data • Service Offers that properly protect client data	• Outperform competitors • Spawn New Business
Develop enterprise-wide dynamic cyber capabilities	• Evaluate tooling chosen for specific areas of use and apply across other entities and practices to leverage skills, training, and value • Leverage internal services like System Monitoring, Incident Response, and Threat Intelligence to offer solutions	• Managed Security Operations Center (SOC) • Intelligence reporting • Asset management	• Spawn New Business
Build organizational agility with cybersecurity	• Integrate cybersecurity aspects of disparate parts of the company, R&D, IT, Factory Operations, and Project Delivery organizations with common policies, controls, governance, and skills	• Secure by Design products • Consistent testing methods with common metrics protect digital-based offers and internal environments	• Outperform competitors • Spawn New Business

Case Study #2 Apple: Differentiating Products and Services with Cybersecurity

Apple has embraced cybersecurity for competitive advantage with a strategic, enterprise focused approach to achieve staying power. Beginning at the hardware level, Apple leverages unique hardware capabilities by incorporating Secure Enclave functionality into their M1 Chip and their T2 Security Chip, achieving economies of scope across their entire catalog of devices. Apps, which are a crucial part of the platform business model, are understood to present the greatest vulnerability to the security of the ecosystem and are "sandboxed" to provide tight controls. Access between apps and users is carefully mediated. Layers of protection are incorporated into the platform to ensure apps are not tampered with and are free of known malware. This reduces the cost to operate the App Store and differentiates their devices in the marketplace. Contrast this cybersecure approach with the Google Play Store. Google does not have a thorough and secure review system, resulting in substantial malware upload. This has become such a costly problem that Google has created an App Defense Alliance to partner with firms in order to detect malware (Doffman, 2019).

Apple introduced services to complement their platform while protecting user privacy and securing user data. Services like iCloud, Find My and Apple Pay created new ways for Apple to outperform rivals. Apple's most recent iPhone operating system iOS 15, in conjunction with their iCloud+ features Private Relay and Hide My Email, has transformed industry structure. Private Relay hides the user's IP address and Safari browsing activity from ISPs and websites (Apple, 2023). These changes reverberated across the industry, For example, Meta experienced $10 billion in lost sales and Google announced they will invest in similar privacy changes over the next two years (Wakabayashi, 2022).

The robustness of Apple's secure devices, platforms, and services enabled them to form a strategic partnership with Cisco, Aon and Allianz to create a holistic cyber risk management solution in response to market pull. This strategic partnership spawned a new business venture: Apple Business Essentials, a subscription-based services offering that allows small businesses to outsource their device management, 24/7 IT support services and secure cloud storage. This partnership also diminishes the threat of new entrants, the threat of substitutes, and the bargaining power of customers. Apple has embraced cybersecurity as a core strategic capability throughout their ecosystem, building agility to seize opportunities and respond to changing markets. Apple's cybersecurity gives them staying power!

Table 2: Apple's Cybersecurity Strategy for Differentiation (Apple.com, 2023)

Strategy	Cybersecurity Strategy	Sample Apple Offerings	Competitive Outcomes

Stratify Cybersecurity across commercial offerings	• Secure Enclave: cybersecurity at the hardware level. • Data Vault mediates and restricts access to data and apps. Devices come with services provide data and pw storage, authentication, payment, etc. while protecting privacy and securing data.	• M1 Chip • T2 Security Chip • App Store • iOS Security • iCloud • Find My • Apple Pay • Sign in with Apple	• Restructure industries • Outperform competitors
Embed cybersecurity across the scope of the organization	• Uses enterprise approach to target cybersecurity investments across the entire Apple ecosystem allowing multiple products to leverage cybersecurity investments • Strategic partnership with Cisco, Aon and Allianz for holistic cyber risk management solutions in response to market demands (Wakabayashi, 2022).	Products • M1 Chip • T2 Security Chip Platforms • App Store • iOS Security Services • iCloud • Find My • Business Essentials	• Spawn new business
Develop enterprise-wide dynamic cyber capabilities	Leverages unique h/w capabilities to control access to sys resources in Apple devices, encompassing boot-up process, software updates and protection of sys resources	• Data Protection • FileVault	• Restructure industries • Outperform competitors
Build organizational agility with cybersecurity	Cybersecurity as a core capability and an ecosystem approach creates tremendous flexibility to respond to changing market demands.	• Strategic partnership • iOS15 • Apple Business Essentials	• Outperform competitors • Spawn new business

Case Study #3 Amazon: Creating a New Secure Cloud Industry

Amazon's e-commerce platform transformed the retail industry and created the secure cloud computing industry, largely due to its embrace of cybersecurity. The early investments into secure, scalable computing infrastructure prevented Amazon from collapsing under hypergrowth (Miller, 2016), allowing their secure ecommerce platform to grow exponentially. The secure infrastructure undergirding operations creates tremendous agility to respond to market forces, evidenced by continuous growth across multiple industries.

With each new security capability Amazon creates, they identify new services that can be offered to clients. Amazon's strategic approach to cybersecurity in their scalable cloud infrastructure allowed them to respond to the pull of the market from clients like the NSA and Nasdaq whose need for secure infrastructure rivaled Amazon's own, spawning a new business for Amazon – Amazon Web Services – which launched in 2006. The strategic approach to develop a secure infrastructure delivered not just economies of scale, but enormous economies of scope that extend across not only Amazon's organization, but out beyond Amazon into organizations in every industry in the world, allowing them to outperform their competitors in multiple industries. Amazon's cybersecurity gives it tremendous staying power!

Table 3: Amazon's Cybersecurity Strategy Created a New Industry (Amazon.com, 2023)

Strategic Principle	Cybersecurity Strategy	Sample Amazon Offerings	Competitive Outcomes

Stratify Cybersecurity across commercial offerings	• Free security token for AWS
	• Created secure, scalable infrastructure to support e-commerce business, facilitating massive platform growth.
		• Products
		  ○ MFA device
		• Platforms
		  ○ E-commerce website
			• Restructure industries
			• Outperform competitors

	Investment led to creation of AWS and secure cloud industry. • AWS led to an ecosystem of third-party security offerings. • AWS leverages internal expertise to create numerous security services to enhance platform.	○ AWS ○ AWS Marketplace • Services ○ Ident Management ○ Threat Detection ○ Infrastructure protection ○ Incident response	• Spawn new business
Embed cybersecurity across the scope of the organization	• Secure infrastructure creates economies of scope across all ops • Transition to cloud across industry verticals created demand for secure, scalable infrastructure. Internal, strategic cybersecurity investments let Amazon respond.	• E-commerce website • AWS	• Outperform competitors • Spawn new business
Develop enterprise-wide dynamic cyber capabilities	Secured the Amazon e-commerce platform by developing numerous core capabilities related to cybersecurity, which are extended into AWS business to create service offerings for clients.	• Secure network, infrastructure, host, and endpoint, data protection/encryption • Logging, monitoring, threat detection and analytics	• Restructure industries • Outperform competitors • Spawn new business
Build organizational agility with cybersecurity	Secure, scalable infrastructure enables tremendous flexibility, allowing Amazon to expand their marketplace, vertically integrate their supply chain, support hypergrowth and create a new business.	• Secure network, infrastructure, host, and endpoint, data protection/encryption • Logging, monitoring, threat detection and analytics	• Restructure industries • Outperform competitors • Spawn new business

Conclusion

In this article, we provide an evidence-based way for strategists to change their perception of cybersecurity as necessary for risk management, but of little value to organizational strategy. Our evidence suggests that not only is cybersecurity a necessary investment to mitigate risk, but that cybersecurity investments can reduce costs and create differentiation in the market – the very definition of competitive advantage (Porter, 1979). Synthesizing the Porter and Cusumano theories we identified four strategies to achieve a competitive advantage with cybersecurity investment and found several actions that executives can explore today.

- ***Differentiate by using cybersecurity to offer increased privacy and security to customers.*** When the need to do secure business increases, so does the payoff for the most secure market leader. Be the industry disruptor by offering cybersecurity to eclipse the competition.
- ***Reduce costs by developing solutions to secure core business processes instead of computers.*** Investing to secure your critical business processes and reduce the risk and impact of a breach can build resilience and reduce the cost of doing business by reducing down time after a breach.
- ***Build strategic alliances to reduce cyber risk.*** Strong partnerships can help with differentiation. Alliances can help build your resilience during an attack. They can lead to new offerings or grant entry to new industries. This can create advantage over market rivals, *and* against new cyber competitors.
- ***Invest in cybersecurity throughout your entire enterprise, from product, to platform, to services, to processes, to capabilities.*** Approaching cybersecurity as part of your corporate platform, building it into products and processes, and extending it into your supply chain is powerful.

Porter's and Millar's (1985) observations are as relevant in 2023 as they were when IT first began to transform businesses. In the light of rapid change, IT could not remain the exclusive territory of the IT department, but needed to be approached strategically in order to leverage it for competitive advantage.

The same can be said for cybersecurity, which, as this research demonstrates, has great potential. And that changes the conversation from infrastructure investment to strategic business opportunity.

References

Amazon. (2023). AWS Cloud Security. https://aws.amazon.com/security/.

Apple. (2023). Apple Business Services and Apple Platform Security. https://www.apple.com/.

Baran B.E., and Woznyj, H.M. (2021). Managing VUCA: The human dynamics of agility. *Organizational Dynamics* (50*), 1-11.*

Brandl, R. (2022). The Most Popular Video Call Conferencing Platforms Worldwide. *Email Tool Tester*. https://www.emailtooltester.com/en/blog/video-conferencing-market-share/.

Chaturvedi, A. (2021). WhatsApp's new privacy policy 'very confusing': Signal's Brian Acton. *The Economic Times*. https://economictimes.indiatimes.com/tech/tech-bytes/whatsapp-new-privacy-policy-very-confusing-signal-cofounder-brian-acton/articleshow/80260743.cms.

Christensen, C.M. (2001). The Past and Future of Competitive Advantage. *MIT Sloan Management Review, 42(2), 105-109*.

Cusumano, M.A. (2010). *Staying Power: Six Enduring Principles for Management Strategy and Innovation in an Uncertain World*, Oxford, United Kingdom: Oxford University Press.

Dillon, S., and Taylor, H. (2015). Employing Grounded Theory to Uncover Behavioral Competencies of Information Technology Project Managers. *Project Management Journal*, 90-104.

Doffman, Z. (2019). Google Enlists Outside Help to Clean Up Android's Malware Mess. *Wired*. https://www.wired.com/story/android-malware-app-defense-alliance/

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed- the-world/.

Hepfer, M., and Powell, T.C. (2020). Make Cybersecurity a Strategic Asset. *MIT Sloan Management Review, 62(1), 40-45*.

Islam, Md. Shariful and Stafford, T. (2017). Information Technology (IT) Integration and Cybersecurity/Security: The Security Savviness of Board of Directors. *AMCIS 2017 Proceedings*.

Miller, R. (2016). How AWS Came to Be. *Tech Crunch* (July 2, 2016). https://techcrunch.com/2016/07/02/andy-jassys-brief-history-of-the-genesis-of-aws/

Newbert, S.L. (2008). Value, Rareness, Competitive Advantage, and Performance: A Conceptual-Level Empirical Investigation of the Resource-Based View of the Firm. *Strategic Management Journal, 29(7), 745-768*.

Pearlson, K. and Huang, K. (2022). Design for Cybersecurity from the Start. *MIT Sloan Management Review*. https://sloanreview.mit.edu/article/design-for-cybersecurity-from-the-start/.

Porter, M.E. (1979). How Competitive Forces Shape Strategy. *Harvard Business Review, 57(2), 137–145*.

Porter, M.E., and Millar, V.E. (1985). How Information Gives You Competitive Advantage. *Harvard Business Review, 63(4), 149-160*.

Ridder, H.G., Hoon, C., and Baluch, A.M. (2014). Entering a Dialogue: Positioning Case Study Findings towards Theory. *British Journal of Management (25),* 373-387.

Schwartz, T., Schuff, D., and Wray, M. (2019). A Dynamic Cyber-Based View of the Firm. *AMCIS 2019 Proceedings*, Association for Information Systems, Cancun, Mexico.

Team at Slack. (2020). "Introducing powerful new layers of enterprise-grade security," *Slack.com*. https://slack.com/blog/transformation/introducing-new-layers-of-enterprise-grade-security.

Wakabayashi, D. (2022). Google Plans Privacy Changes, but Promises to Not Be Disruptive. *The New York Times*. https://www.nytimes.com/2022/02/16/technology/google-android-privacy.html.