radware

MANAGING REAL-WORLD RISKS

WHAT CAN WE LEARN ABOUT CYBERSECURITY FROM THE CHALLENGER DISASTER? EVERYTHING.

Understanding the potential threats that your organization faces is an essential part of risk management in modern times. It involves forecasting and evaluating all the factors that impact risk. Processes, procedures and investments can all increase, minimize or even eliminate risk.

Another factor is the human element. Often times, within an organization, a culture exists in which reams of historical data tell one story, but management believes something entirely different. This "cognitive dissonance" can lead to an overemphasis and reliance on near-term data and/or experiences and a discounting of long-term statistical analysis.

Perhaps no better example of this exists than the space shuttle Challenger disaster in 1986, which now serves as a case study in improperly managing risk. In January of that year, the Challenger disintegrated 73 seconds after launch due to the failure of a gasket (called an O-ring) in one of the rocket boosters. While the physical cause of the disaster was caused by the failure of the O-ring, the resulting Rogers Commission that investigated the accident found that NASA had failed to correctly identify "flaws in management procedures and technical design that, if corrected, might have prevented the Challenger tragedy."

Despite strong evidence dating back to 1977 that the O-ring was a flawed design that could fail under certain conditions/temperatures, neither NASA management nor the rocket manufacturer, Morton Thiokol, responded adequately to the danger posed by the deficient joint design. Rather than redesigning the joint, they came to define the problem as an "acceptable flight risk." Over the course of 24 preceding successful space shuttle flights, a "safety culture" was established within NASA management that downplayed the technical risks associated with flying the space shuttle despite mountains of data, and warnings about the O-ring, provided by research and development (R & D) engineers.

As American physicist Richard Feynman said regarding the disaster, "For a successful technology, reality must take precedence over public relations, for nature cannot be fooled."

Truer words have never been spoken when they pertain to cybersecurity. C-suite executives need to stop evaluating and implementing cybersecurity strategies and solutions that meet minimal compliance and establish a culture of "acceptable risk" and start managing to real-world risks — risks that are supported by hard data.

RISK MANAGEMENT AND CYBERSECURITY

The threat of a cyberattack on your organization is no longer a question of if, but when, and C-suite executives know it. According to *C-Suite Perspectives: Trends in the Cyberattack Landscape, Security Threats and Business Impacts*, 96% of executives were concerned about network vulnerabilities and security risks resulting from hybrid computing environments. Managing risk requires organizations to plan for and swiftly respond to risks and potential risks as they arise. Cybersecurity is no exception. For any organization, risks can be classified into four basic categories:

Strategic Risk
A risk that is affected or created by strategy decisions

Reputation Risk
A risk that involves the public reputation of the organization and affects its ongoing success.

Product Risk
A risk that arises due to a product being poorly designed, lacking quality or failing to meet customers' expectations

Govenance Risk
A risk that considers control/ management approaches that direct an organization and control the manner in which it's governed

The Challenger disaster underscores all four of these risk categories. Take strategic risk as an example. Engineers from Morton Thiokol expressed concerns and presented data regarding the performance of the O-rings, both in the years prior and days leading up to the launch, and stated the launch should be delayed. NASA, under pressure to launch the already delayed mission and emboldened by the 24 preceding successful shuttle flights that led them to discount the reality of failure, pressured Morton Thiokol to supply a different recommendation. Morton Thiokol management decided to place organizational goals ahead of safety concerns that were supported by hard data. The recommendation for the launch was given, resulting in one of the most catastrophic incidents in manned space exploration. Both Morton Thiokol and NASA made strategic decisions that placed the advancements of their respective organizations over the risks that were presented.

This example of strategic risk serves as a perfect analogy for organizations implementing cybersecurity strategies and solutions. There are countless examples of high-profile cyberattacks and data breaches in which upper management was warned in advance of network vulnerabilities, yet no actions were taken to prevent an impending disaster. The infamous 2018 Panera Bread data breach is one such example. Facebook is yet another. Its platform operations manager between 2011 and 2012 warned management at the social tech giant to implement audits or enforce other mechanisms to ensure user data extracted from the social network was not misused by third-party developers and/or systems. These warnings were apparently ignored.[1]

So why does this continually occur? The implementation of DDoS and WAF mitigation solutions often involves three key components within an organization: management, the security team/SOC and compliance. Despite reams of hard data provided by a security team that an organization is either currently vulnerable or not prepared for the newest generation of attack vectors, management will often place overemphasis on near-term security

1 https://www.cnet.com/news/facebook-ignored-data-breach-risks-ex-employee-sandy-parakilas-says/

results/experiences; they feel secure in the fact that the organization has never been the victim of a successful cyberattack to date. The aforementioned Facebook story is a perfect example: They allowed history to override hard data presented by a platform manager regarding new security risks.

Underscoring this "cognitive dissonance" is the compliance team, which often seeks to evaluate DDoS mitigation solutions based solely on checkbox functionality that fulfills minimal compliance standards. Alternatively, this strategy also drives a cost-savings approach that yields short-term financial savings within an organization that often times views cybersecurity as an afterthought vis-à-vis other strategic programs, such as mobility, IoT and cloud computing.

The end result? Organizations aren't managing real-world risks, but rather are managing "yesterday's" risks, thereby leaving themselves vulnerable to new attack vectors, IoT botnet vulnerabilities, cybercriminals and other threats that didn't exist weeks or even days ago.

THE TRUE COST OF A CYBERATTACK

To understand just how detrimental this can be to the long-term success of an organization requires grasping the true cost of a cyberattack. Sadly, these data points are often as poorly understood, or dismissed, as the aforementioned statistics regarding vulnerability. The cost of a cyberattack can be mapped by the four risk categories.

1 STRATEGIC RISK	Cyberattacks, on average, cost more than one million USD/EUR, according to 40% of executives. Five percent estimated this cost to be more than 25 million USD/EUR.[2]
2 REPUTATION RISK	Customer attrition rates can increase by as much as 30% following a cyberattack. Moreover, organizations that lose over four percent of their customers following a data breach suffer an average total cost of $5.1 million.[3] In addition, 41% of executives reported that customers have taken legal action against their companies following a data breach.[2] The Yahoo and Equifax data breach lawsuits are two high-profile examples.
3 PRODUCT RISK	The IP Commission estimated that counterfeit goods, pirated software and stolen trade secrets cost the U.S. economy $600 billion annually.[4]
4 GOVERNANCE RISK	"Hidden" costs associated with a data breach include increased insurance premiums, lower credit ratings and devaluation of trade names. Equifax was devalued by $4 billion by Wall Street following the announcement of its data breach.[5]

2 *C-Suite Perspectives: Trends in the Cyberattack Landscape, Security Threats and Business Impacts*
3 https://www.journalofaccountancy.com/news/2016/jul/hidden-costs-of-data-breach-201614870.html
4 http://ipcommission.org/press/IPC_press_release_030818.pdf
5 http://time.com/money/4936732/equifaxs-massive-data-breach-has-cost-the-company-4-billion-so-far/

MANAGE REAL-WORLD RISKS BY SECURING THE CUSTOMER EXPERIENCE

It's only by identifying the new risks that an organization faces each and every day and having a plan in place to minimize them that enables its executives to build a foundation upon which their company will succeed. In the case of the space shuttle program, mounds of data that clearly demonstrated an unacceptable flight risk were pushed aside by the need to meet operational goals. What lessons can be learned from that fateful day in January of 1986 and applied to cybersecurity? To start, the disaster highlights the five key steps of managing risks.

Five Key Steps of Managing Risks

1. IDENTIFY RISKS EARLY AND OFTEN
2. ANALYZE AND TRUST THE DATA
3. CONTROL MITIGATION FACTORS
4. TRANSFER RISK
5. CONDUCT A POST-ANALYSIS AND MEASURE THE RESULTS

In the case of cybersecurity, this means that the executive leadership must weigh the opinions of its network security team, compliance team and upper management and use data to identify vulnerabilities and the requirements to successfully mitigate them. In the digital age, cybersecurity must be viewed as an ongoing strategic initiative and cannot be delegated solely to compliance. Leadership must fully weigh the potential cost of a cyberattack/data breach on the organization versus the resources required to implement the right security strategies and solutions. Lastly, when properly understood, risk can actually be turned into a competitive advantage. In the case of cybersecurity, it can be used as a competitive differentiator with consumers that demand fast network performance, responsive applications and a secure customer experience. This enables companies to target and retain customers by supplying a forward-looking security solution that seamlessly protects users today and into the future.

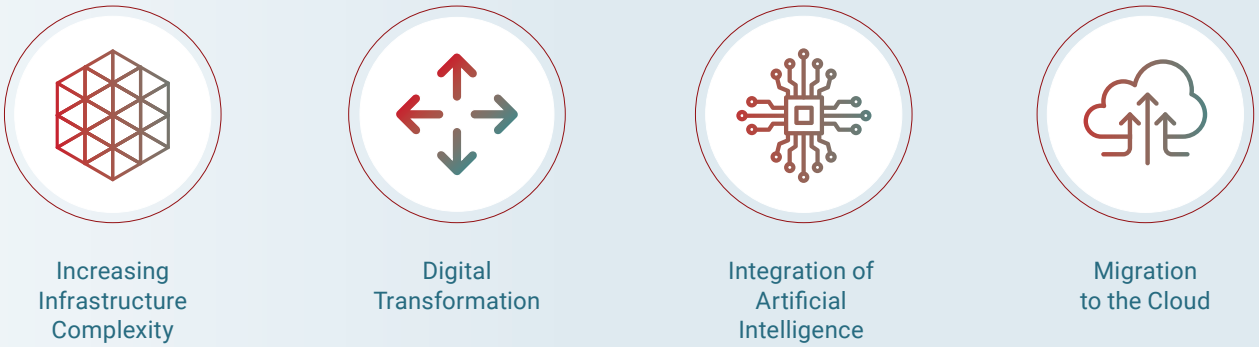
So how are executives expected to accomplish this while facing new security threats, tight budgets, a shortfall in cybersecurity professionals and the need to safeguard increasingly diversified infrastructures? The key is creating a secure climate for the business and its customers.

To create this climate, research shows that executives must be willing to accept new technologies, be open-minded to new ideologies and embrace change, according to *C-Suite Perspectives: Trends in the Cyberattack Landscape, Security Threats and Business Impacts*. Executives committed to staying on top of this ever-evolving threat must break down the silos that exist in the organization to assess the dimensions of the risks across the enterprise and address these exposures holistically. Next is balancing the aforementioned investment versus risk equation. All executives will face tough choices when deciding where to invest resources to propel their companies forward. C-suite executives must leverage the aforementioned data points and carefully evaluate the risks associated with security vulnerabilities and the costs of implementing effective security solutions to avoid becoming the next high-profile data breach.

According to the same report, four in 10 respondents identified increasing infrastructure complexity, digital transformation plans, integration of artificial intelligence and migration to the cloud as events that put pressure on security planning and budget allocation.

Balancing Investments Versus Risk

Risk management calculations affect security investments.
Four in 10 said that these factors put pressure on security planning and budgets.



The stakes are high. Security threats can seriously impact a company's brand reputation, resulting in customer loss, reduced operational productivity and lawsuits. C-suite executives must heed the lessons of the space shuttle Challenger disaster: Stop evaluating and implementing cybersecurity strategies and solutions that meet minimal compliance and start managing to real-world risks by trusting data, pushing aside near-term experiences/"gut instincts" and understanding the true cost of a cyberattack. Those executives who are willing to embrace technology and change and prioritize cybersecurity will be the ones to win the trust and loyalty of the 21st-century consumer.