radware

THE MILLION-DOLLAR QUESTION OF CYBER-RISK:

INVEST NOW OR PAY LATER?

Cybersecurity is often an afterthought. Executives are quick to focus on the endgame benefits of customer-centric strategies, digital transformation, mobility, IoT and cloud computing, yet cybersecurity often falls by the wayside compared to these strategic initiatives. In fact, many executives view cybersecurity strictly as a cost center.

This cost-savings, bolt-on approach to implementing cybersecurity might yield short-term financial savings that leave the finance department feeling good. But it also leaves organizations in a "pay me now, pay me later" scenario that runs the risk of significant financial loss and damage to customer satisfaction and market reputation in the long run. Resulting breaches devalue and compromise any digital transformation and/or customer-facing programs, resulting in lost time, money and, most importantly, customer faith.

In an increasingly insecure world where security and availability are the cornerstones of the digital consumer, organizations must reevaluate how they balance the investment versus risk equation and alter how and when they implement cybersecurity.

THE TRUE COST OF A DDoS ATTACK

To understand just how detrimental this approach can be to the long-term health of an organization requires a grasp of the true cost of a DDoS attack. Sadly, these types of statistics are often poorly understood by organizations. According to Radware, 80 percent of organizations don't calculate the cost of cyberattacks.[1] You can't manage what you don't measure.

Ultimately, DDoS attacks are far more expensive than organizations realize. Not only in monetary costs but also by damage incurred to brand reputation, operational expenses and, most importantly, the impact on the customer experience.

As a starting point, DDoS attacks cost, on average, more than 1 million USD/EUR, according to 40 percent of global executives.[2] This figure represents the actual operational costs associated with "cleaning up" an attack. Five percent of executives estimate this cost to be more than 25 million USD/EUR. But these figures only represent the tip of the iceberg.

1 Radware's Global Application & Network Security Report
2 C-Suite Perspectives: Trends in the Cyberattack Landscape, Security Threats and Business Impacts

The larger, more damaging effect is the impact on customer loyalty and trust, brand damage and a wide array of other "hidden costs." According to executives, the top three impacts from a cyberattack are:

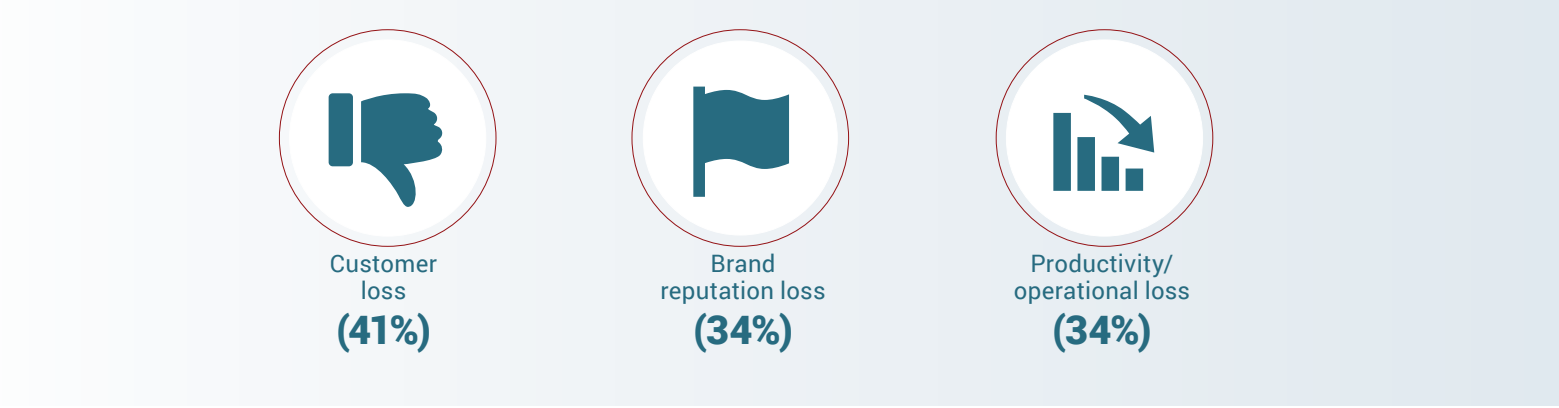

Figure 1: Statistics from C-Suite Perspectives: Trends in the Cyberattack Landscape, Security Threats and Business Impacts

Customer Loss – In today's digitally driven world where consumers own the relationship, the foundation of the customer experience is a mix of security and availability. Customer attrition rates can increase by as much as 30 percent following a successful cyberattack.

Revenue Loss - Shopping cart abandonment, no product inventory, increased bounce rates...these are all byproducts of successful DDoS attacks that can result in revenue loss.

Productivity/Operational Loss - The inability to access email, critical business applications, and company networks, can directly impact productivity.

Impact to the Digital Experience - DDoS attacks create service degradation or complete outages, breaking hard-earned customer trust and undermining the aforementioned digital transformation and customer-centric strategies executives are so keen to implement.

Lastly, emergency onboarding of a DDoS mitigation solution during an attack is costly, difficult and takes away control from security teams. Few resources, either internal or from your organization's ISP, are available during an attack to handle the onboarding process. Lastly, onboarding can take several days, leaving your organization vulnerable during that time period.

FLIP THE PARADIGM

What if organizations could flip the paradigm? What if organizations could create a secure environment for their customers and, in the process, use security as a competitive differentiator?

The impact on businesses is twofold. Whereas companies were once reticent to speak publicly about cybersecurity because it could cause consumers to question their business's fragility, they must now embrace and communicate their ability to safeguard customer data. Forward-thinking organizations must use security and due diligence as competitive differentiators to build trust and loyalty with customers in the face of an increasingly insecure world.

It is no longer about delivering a world-class experience. It is about delivering a SECURE, world-class experience. In today's digitally driven, social media world where consumers own the relationship, security has to become the very fabric of the business.

So how are executives expected to accomplish this 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 customers by embracing technology and change. Corporate networks are the linchpins of interactions with customers who expect responsive apps, fast performance and, above all, protection of their data.

Balancing Investment and Risk

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

1. INCREASING INFRASTRUCTURE COMPLEXITY
2. DIGITAL TRANSFORMATION
3. INTEGRATION OF ARTIFICIAL INTELLIGENCE
4. MIGRATION TO THE CLOUD

Figure 2: Statistics from 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. As the threat of cyberattacks becomes a question of when, not if, 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.

Learn more about which DDoS protection model would meet your organization's financial and technological needs