Are Businesses Shortchanging Cybersecurity Or Shortchanging Change Itself?

At a recent private gathering of cybersecurity professionals, I watched how the conversation gravitated toward an analysis of two interesting facts: First, according to a survey commissioned by Gartner (paywall), businesses are increasing their cybersecurity budgets at a rate of 18%; second, data breaches increased at a rate of more than 40% from 2015 to 2016, based on a Bloomberg report.

From a financial point of view, we're getting a questionable return on our security investments. It begs the question: Are we investing enough in cybersecurity, or are the investments we're making not optimal? One way or another, businesses will need to close the cyber-readiness gap or become increasingly vulnerable to cyberthreats.

Responding To Change

For several reasons, we've arrived at a moment in history when businesses -- to borrow a line from Apple -- need to "think different" about their investments in cybersecurity.

Business is driving a rapid change in the technology landscape. The cloud is providing the enterprise with immense value by providing greater access to information, services, customers, partners and employees while radically lowering the costs of services, transactions and communications. Additionally, the enterprise has embraced technologies to increase mobility, empower employees, enhance partnerships and strengthen customer relationships while accepting the growing roles that personal devices and social media are playing in business. This has challenged the traditional security models that most enterprises have leveraged to protect themselves.

The change in enterprise IT is both obvious and profound. Yet the way we make decisions for investing in security has not changed much at all over the last 20 years. Part of the problem is institutional. Industry frameworks that many enterprises have adopted -- like ISO 27001/27002 -- look at cybersecurity through a highly segmented lens, leading to the creation and adoption of many point solutions that sometimes overlap and that often fail to address the changing realities of the evolution taking place across the technology landscape. In addition, the frameworks don't allow for evaluating strategic investment tradeoffs or provide risk professionals with a long-term view of the problem.

There's another type of pressure that reinforces short-sighted thinking: Many security investments decisions are driven by events, compliance requirements and a plethora of vendors selling point solutions to address one pain point or another. The problem? Security decisions are not driven by understanding strategic investment tradeoffs, the long-term value of your cyber-risk investments or even holistically addressing the massive transformation taking place in technology.

Investing In Change

What's becoming increasingly apparent is that current security frameworks and point solutions are getting in the way of the serious work that needs to be done to safely prepare businesses to thrive in the digital age. The transformation taking place in technology demands that businesses reshape their security infrastructures. Yet rapid technology transformation can make our security investments obsolete or quickly reduce their effectiveness as a security control. Value from security investments today does not mean we obtain that value tomorrow. Transforming our security capabilities, just like the technology transformation, will require numerous years of investments in security solutions that address the long-term security challenges facing enterprises.

What's also becoming clear is that most businesses lack an investment model for managing cyber risk over time. Given there are a plethora of ways of addressing any identified risks or threats (mobile device management, encryption software, application security, etc.), and there are an increasing number of risks and threats that need to be addressed, the methodology an organization uses to decide what it invests in is very important.

Ideally, the enterprise should analyze security strategy and investments across three horizons:

- **Current State Horizon**: This will help understand how potential security capabilities address immediate risks or deficiencies that exist today.

- **Business Horizon**: This is to review an organization's business strategy, business actions, and business investments and understand how potential security investments will align, support and enable the business.

- **Disruptive Technology Horizon**: This is to show how potential security investments choices address disruptive technology trends -- the growth of IoT, for example -- that will potentially disrupt an organization's security model.

Most organizations just focus on the Current State Horizon while failing to address the more forward-looking horizons. In a time of accelerating change, investing in security means investing in the future.

In the articles to follow in this series, I will develop the contours of an investment model for managing cyber risk by looking at the new frameworks, services and technologies required to protect the modern enterprise today and tomorrow. I will do this against the backdrop of emerging business technology trends and the inevitable next wave of cyberattacks in both the public and private sectors. I will do this in the context of long-term potential technology disruptions, looking at several innovations in their infancy that may ultimately result in the unforeseen black swan. In the end, I will come back to the first question posed in the title of this first article: Are businesses shortchanging cybersecurity?

My hunch: Many businesses are not so much shortchanging their investments but shortchanging their investment in change itself. That could pose a greater threat to businesses than the short-term risks that threaten them today.