KPMG

Transforming companies must put cyber security front and center

Global Cyber Security

KPMG International

kpmg.com/frontandcenter

Cyber preparedness can be a growth driver for transforming companies

When it comes to cyber security, far too many executives are missing the 'big picture.' It's a blind spot that threatens to cost their companies billions.

Greg Bell
Co-Leader, Global Cyber Security
KPMG International
E: rgregbell@kpmg.com

Greg serves as a Co-Leader for the Global Cyber Security practice and a Principal in the US member firm. He has extensive experience helping global Fortune 500 companies protect their critical business information by helping to align their most important business processes with supporting technologies and foundational risk management elements.

Virtually every business competing in today's dynamic market environment — regardless of size, sector, or past success — is on a transformation journey. Customer behaviors and expectations, and a multitude of technologies are forcing senior executives to re-think their organizations' traditional business and operating models. At KPMG, Cyber Security professionals working in member firms around the globe believe that cyber security must be front and center.

The introduction of disruptive technologies and the evolution of customers' expectations mean that the extent of connectivity and the volume of sensitive data accessible about your business and your customers are growing at an exponential rate — leading to great opportunities and risks for your organization. When you hear the term 'cyber security', there's a very good chance that, like many executives, you immediately think of one thing: an IT infrastructure challenge.

Of course, a strong IT security infrastructure is a critical part of any cyber security program. However, it is not the only part. In a 2017 world, this traditional 'defense-first' mindset is too limited and can actually hinder your company's long-term growth prospects. Indeed, there is another important element at play and that is the potential impact of cyber under-preparedness to your company's future business growth. This is particularly true in a business environment in which so many companies are undertaking ambitious customer-focused transformation programs amid widespread technological disruption and competitive threats.

KPMG's Cyber Security professionals are confident that tomorrow's leading businesses will ultimately wield their cyber security capabilities as competitive advantages. Cyber security solutions are a core value proposition to customers to drive growth, and a necessity for management teams, board members, and investors to continue making investments in technology-enabled transformations. Without confidence in cyber security solutions from all of these stakeholders, organizations limit their ability to innovate business and operating models, leading to current customer defection and poor growth prospects.

KPMG's 2016 Global CEO Outlook study confirmed that the next 3 years are going to be incredibly transformative for global companies. A majority of CEOs (77 percent) said that 'innovation' will be a core component of their business strategies over that period. Perhaps most surprising of all, however, was the finding that 68 percent of CEOs who describe their companies as being 'less prepared for a cyber event' stated that they thought the next 3 years would be more critical for their businesses than the previous 50.

The pace of change continues to accelerate as the fourth industrial revolution ushers in an era of machine learning, cognitive computing, artificial intelligence and a world in which virtually everything is connected through the internet of things. Amid these rapid technological advances, the associated

77 percent of CEOs say that ‘innovation’ will be a core component of their business strategies over the next 3 years.

security risks are also increasing exponentially. In October 2016, the world caught a glimpse of those risks when hackers used tens of thousands of compromised internet of things devices (e.g. cameras, routers and DVRs) to launch distributed denial of service attacks that caused widespread internet problems and disrupted access to a host of popular online services*.

We’re living in a world in which technological change is taking place at lightning speed, companies are transforming and everything is connected. The bottom line for CEOs of transforming companies is that they and their leadership teams need to act now to implement a strategic, holistic approach to cyber preparedness that will not only protect their valuable data, but also enhance the company’s agility and better position it for growth down the road.

Most companies have some perception of the risk side of the cyber equation. In other words, if we don’t do this and we have a breach, we will lose customers, it will negatively impact our brand, etc. But there’s also a positive aspect to this equation. Cyber preparedness can actually enable your company for new opportunities for revenue growth. That should be the message that more CEOs are listening to today.

Many executives and directors have anxiety around adopting new technologies to gain a competitive advantage. Every week I have conversations with board members who say they’re concerned about putting their information ‘in the cloud’ and that they think it means they can get attacked more easily. What I tell them is that number one, most cloud service providers understand security is a priority and they build their systems accordingly. And number two, I remind them that sometimes not moving to the cloud is a bigger risk than putting your information there. If all of your competitors are in the cloud, they’re able to be faster and more agile. By staying with your legacy, slow-moving IT infrastructure, you can be putting your company at a distinct competitive disadvantage. In other words, the value you can provide to your customers can be limited by your technology stack.

One of the other major blind spots for executives is viewing cyber security as an IT risk only, when it should really be viewed as a strategic part of the company’s holistic business strategy. The question shouldn’t be ‘how much of my IT budget are we spending on cyber’. The question should be ‘how much of my business change or innovation budget are we spending on cyber security?’ When you treat cyber security as an IT risk only, you risk missing opportunities and inflection points that could help fuel business growth.

Cyber preparedness enables your company to focus on new opportunities for revenue growth

* ‘3rd Cyberattack ‘Has Been Resolved’ After Hours of Major Outages: Company’ | News | nbcnewyork.com | 21 October 2016 | http://www.nbcnewyork.com/news/local/Major-Websites-Taken-Down-by-Internet-Attack-397905801.html

When you treat cyber security as an IT risk only, you risk missing opportunities and inflection points that could help fuel business growth.

No matter what industry you're in, data is the lifeblood of modern business. A high-quality cyber preparedness program will not only focus on keeping the data safe and secure. It will also help to increase and improve the integrity of that data to make sure that you have the right and complete data upon which to base your business decisions.

Recently, an equipment manufacturer with a long track record of strong sales and premium pricing noticed that they were losing market share. Their analysis revealed that their products were having a much higher fail rate than usual. As a result, an increasing number of customers were opting to buy from other competitors. After further investigation, the company realized it had actually been the subject of a cyber attack. However, this wasn't a typical breach in which customer or company information was stolen. Instead, the hackers had gone in and changed the parameters in the company's quality control programs so that every component (even those with flaws and defects) would pass quality control testing. Their operational systems were telling them everything was fine. Meanwhile, they were sending sub-par products into the marketplace because a cyber attack had impacted the integrity of their data. The financial impact of this attack measured in the billions of dollars.

In another example, a major retailer suffered a cyber attack in which customer information was stolen by hackers. The breach resulted in negative headlines, a falling stock price, a tarnished brand, executive terminations and lawsuits against the board. Those were the tangible, day-to-day business impacts that could be witnessed and measured. What may not have been publicly known was the fact that because the retailer had to deal with the fallout from this massive breach, their business growth program, which had been its number one priority prior to the breach, had to be shelved for 18 months. That growth program would have been a strategic benefit that could have helped the company increase its market share and growth opportunities. And it had to be put on hold for a year and a half due to the hack. While it's difficult to pinpoint the financial impact of that delay, it's fair to say it would have been in the hundreds of millions of dollars.

4 | Transforming companies must put cyber security front and center

In KPMG's 2016 Global CEO Outlook survey, cyber security was the top risk named by global CEOs this year, up from the fifth-highest ranking last year. Despite this level of awareness and concern, 72 percent of CEOs say their companies are not fully prepared for a cyber event.

Companies are hungry for growth. CEOs have told us they're prioritizing innovation at a strategic level. Yet, organizations continue to underinvest in cyber security and this under-preparedness is one of the top barriers to innovation.

In an increasingly connected and fast-paced business environment, leadership teams must look at every major business decision through the cyber security lens. They need to ensure that they have people in all parts of the organization who understand cyber issues. And they need to talk about and plan for these issues up front, so they can understand where the business is going, plan for that change and build a more adaptive, agile cyber security strategy that aligns more closely to the business to help set the stage for security, innovation and growth.

"We're living in a technological time, in which meeting and exceeding your stakeholders' cyber preparedness expectations has become a critical value-driver for business. Cyber security is not just an IT challenge; it has become a core business challenge. Your stakeholders need to feel comfortable that you're protecting the sensitive information. The cyber security solution that you deploy is an integral part of developing your business and operating model strategy and the value propositions that you deliver to your customers."

Stephen G. Hasty, Jr.
Global Transformation Leader
KPMG International

Contact us

Global

Greg Bell
Co-Leader, Global Cyber Security
E: rgregbell@kpmg.com

Akhilesh Tuteja
Co-Leader, Global Cyber Security
E: atuteja@kpmg.com

Americas

Canada

Paul Hanley
Partner and Cyber Security Leader
E: pwhanley@kpmg.ca

United States

Anthony Buffomante
Partner and Cyber Security Leader
E: abuffomante@kpmg.com

Latin America

Leandro Antonio
Partner and Regional Cyber Security Leader
E: lantonio@kpmg.com.br

Asia Pacific

Australia

Gordon Archibald
Partner and Cyber Security Leader
E: garchibald@kpmg.com.au

China and Hong Kong

Henry Shek
Partner and Cyber Security Leader
E: henry.shek@kpmg.com

Japan

Atsushi Taguchi
Partner and Cyber Security Leader
E: atsushi.taguchi@jp.kpmg.com

Singapore

Daryl Pereira
Partner and Cyber Security Leader
E: darylpereira@kpmg.com.sg

Europe, Middle East and Africa

France

Vincent Maret
Partner and Cyber Security Leader
E: vmaret@kpmg.fr

Germany

Uwe Bernd-Striebeck
Partner and Cyber Security Leader
E: uberndstriebeck@kpmg.com

India

Atul Gupta
Partner and Cyber Security Leader
E: atulgupta@kpmg.com

Italy

Luca Boselli
Partner and Cyber Security Leader
E: lboselli@kpmg.it

Netherlands

John Hermans
Partner and EMA Regional Cyber Security Leader
E: hermans.john@kpmg.nl

Nordics

Mika Laaksonen
Partner and Cyber Security Leader
E: mika.laaksonen@kpmg.fi

Spain

Marc Martinez
Partner and Cyber Security Leader
E: marcmartinez@kpmg.es

Switzerland

Matthias Bossardt
Partner and Cyber Security Leader
E: mbossardt@kpmg.com

United Kingdom

Paul Taylor
Partner and Cyber Security Leader
E: paul.taylor@kpmg.co.uk

Saudi Arabia

Manhal M. Musameh
Head of IT Advisory
E: mmusameh@kpmg.com

kpmg.com/cybersecurity
kpmg.com/transformation

kpmg.com/socialmedia

Publication name: Transforming companies must put cyber security front and center

Publication number: 133922-G
Publication date: March 2017