KPMG

Privately Speaking

Insights on private company growth from private company insiders

Issue 57 | Strengthening your business | August 2019

Cyber in an evolving marketplace

Cybersecurity is at the top of the agenda—for CEOs, for customers, and for investors. Yet, most private market CEOs admit that they are underprepared for the inevitable. With trust hanging in the balance, this edition of Privately Speaking *shines the spotlight on cybersecurity—the risks, the innovations, and the market demand.*

A looming risk

According to a recent survey of U.S.-based private market CEOs…

of private companies are underprepared for a cyber attack

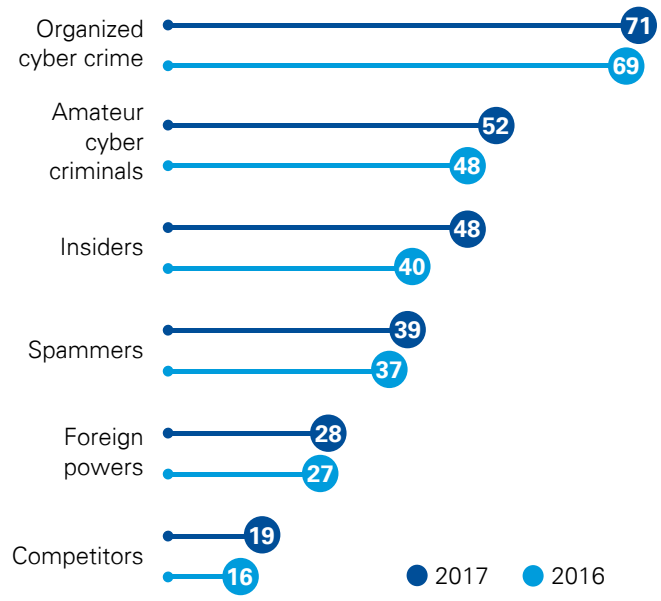
believe that a cyber attack on their organization is inevitable

Source: KPMG 2019 CEO Outlook Survey

While emerging technologies certainly pose a heightened cyber risk, the reality is that most cyber criminals aren't using new technologies to launch new forms of attacks. More often than not, hackers and other bad actors are discovering and attacking system weaknesses that may be a decade or more old.

These vulnerabilities must be addressed. For many private market organizations, the challenge often comes down to a lack of talent/manpower, time, budget, or understanding of the true nature of the threats—typically it is a combination of these challenges.

Bad cyber actors come in many forms—threat origins that CIOs are most concerned about



Value in percentages

Source: Harvey Nash/KPMG CIO Survey 2017

What are the leaders doing?

The best chief information security officers and cybersecurity companies are taking a strategic, business-level view of their cyber risks and defenses, similar to that taken by the attackers themselves. They're stepping back and looking at cybersecurity as an enterprise-wide issue rather than as a single technology problem. They're asking where the greatest assets and risks lie, which areas need the greatest protection, how attackers are most likely to break in, and what the business implications of a breach might be.

The data ecosystem is broad and deep—you must approach security holistically.

> Whether you are a legacy company embracing the cloud or a digital company expanding your products, channels, and services, you need to think pragmatically about your cyber strategy. The risk is rising for every company. The only choice is to be proactive and adaptive while remaining mindful of the overall architecture of your networks.
>
> —**Brian Hughes**, National Private Markets Group Leader and National Venture Capital Coleader, KPMG LLP

No trust without cybersecurity

Privately held companies understand the relationship between cybersecurity and trust.

A strong cyber strategy is critical to engendering trust with our key stakeholders.

Source: KPMG 2019 CEO Outlook Survey

A hot market for investors

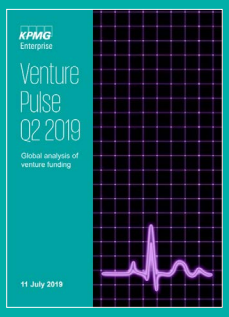
Venture capital (VC) investors recognize the evolving requirements of cybersecurity. In 2018, a record $1.7 billion in VC funding went to cybersecurity across 99 deals. By the end of Q2'19, over $800 million in VC funding was raised by cybersecurity-focused firms.

> Demand for cyber products and services is growing rapidly. And now, with new technologies like deep learning starting to show real promise in the field, VC investors are pouring money into the sector, maintaining a healthy clip of deal-making thus far in 2019.
>
> —**Conor Moore**, National Venture Capital Coleader, KPMG LLP

Want more?

Find out more about recent VC activity in the cybersecurity space in our most recent **Venture Pulse report**.

Read more



Artificial Intelligence to the rescue?

Recently, security professionals have been exploring cognitive technologies and artificial intelligence, particularly deep learning, to better anticipate and defend against cyber threats.

Security professionals have historically dealt with the challenge of "making sense" of the data they collect to shore up their defenses. Deep learning has the ability to correlate numerous data sources to identify patterns or anomalies that might point to malicious activities. Companies are employing deep learning algorithms not only to help them identify security incidents, but also to assess systemwide vulnerabilities.

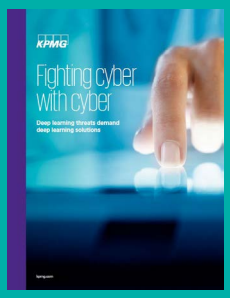
As a cybersecurity tool, deep learning has been making particular progress in three key areas:

— Adversarial sample detection: Hidden neural layers in deep learning can be activated to detect incorrect classifications caused by adversarial attacks.

— Malware detection: Deep learning is being coupled with machine learning to identify and classify malware within enterprise systems.

— Network intrusion detection: Deep learning approaches to managing network security are starting to outperform previous state-of-the-art methods.

Learn more about how cybersecurity leaders are applying deep learning in this **recent report** by KPMG LLP.



Read more

A competitive differentiator?

Many private market companies are using their cybersecurity stance as a way to differentiate.

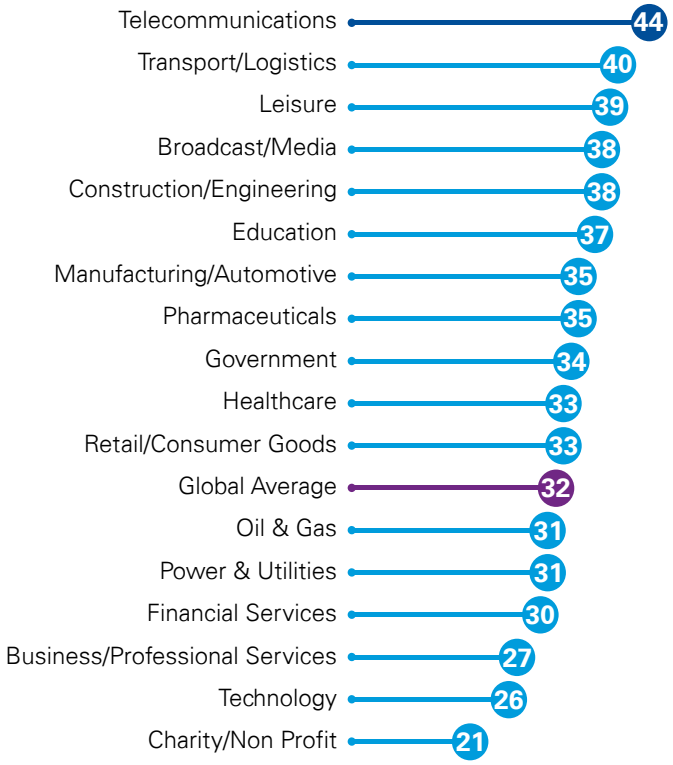
My organization views information security as a strategic function and as a potential source of competitive advantage.

Source: KPMG 2019 CEO Outlook Survey

A call to action

To withstand a cyber attack, private market companies need to have a coordinated enterprise cybersecurity blueprint that looks out over the next three to five years. This framework should incorporate every touchpoint; include strategies for infrastructure, data science talent, internal controls, and governance; and must have the flexibility to accommodate changes, as developments inside and outside the organization demand.

Sectors that experienced a major cyber attack in the last two years



Values in percentages

Source: Harvey Nash/KPMG CIO Survey 2019

How KPMG can help

Cybersecurity is a strategic enterprise risk that goes far beyond IT. Whether we are working with your boardroom, back office, or data center, we seek to provide a jargon-free explanation of your cyber threats, the potential impact to your critical assets, and the recommended response. Ultimately, we view cybersecurity through a cross-functional business lens, encompassing people, change, and financial and risk management. **Learn more**

On the minds of private company CEOs

In addition to matters surrounding cyber, what other critical topics are U.S. CEOs thinking about to ensure their organizations remain resilient? Explore the results of our latest CEO Outlook report for more insight into what's on the minds of private company CEOs. **Read more**

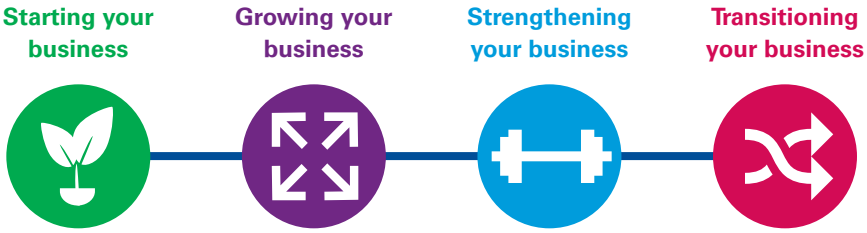
Don't miss a thing

The environment for private companies is changing rapidly, and new opportunities are emerging every day.

Do not let an opportunity pass you by. Sign up to receive KPMG's ***Privately Speaking*** series and make sure you are making the best decisions possible for your private company.

Register here to subscribe to KPMG's *Privately Speaking* series:

Subscribe



Privately Speaking **focuses on the issues that matter most to privately held entities, including PE- and VC-backed companies.**

KPMG's Private Markets Group understands what it takes to drive private company growth. In each edition of ***Privately Speaking***, we share our insights—along with practical and actionable tips—to help boards, executives, and management grow, strengthen, and transition their privately held businesses.

For more information, click here to visit our *Privately Speaking* web page.

Contacts

Brian Hughes
Partner
National Private Markets Group (PMG) Leader
National Venture Capital Coleader
T: 267-256-1820
E: bfhughes@kpmg.com

Conor Moore
Partner
National Venture Capital Coleader
T: 415-963-7559
E: conormoore@kpmg.com

Sal Melilli
Partner
National PMG Audit Leader
T: 212-872-6030
E: smelilli@kpmg.com

Brad Sprong
Partner
National PMG Tax Leader
T: 816-802-5270
E: bsprong@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia