

**Bitdefender**<sup>®</sup>

Virtualization makes  
CIOs role key  
(A survey on US IT decision makers)





## Executive summary:

An October 2016 Bitdefender survey of 250 IT decision makers in the United States in companies with more than 1,000 PCs, shows they will rise in companies' hierarchies, as CEOs and board members face increasing internal and external security risks that could ruin customer trust and business forecasts. Still, not all C-suites include CIOs/CISOs in the business decision-making process. This survey, carried out by iSense Solutions, shows how IT decision makers perceive their role inside the organizations and what they need to meet shareholder expectations. How has virtualization changed the security game? How many attacks can be stopped with the current resources? Would they pay to avoid public shaming?

### Key findings:

- A third of CIOs say their job is more important in the company's hierarchy. Another third even agree their job has been completely transformed in recent years.
- Nine in 10 IT decision makers perceive IT security as a top priority for their companies. However, only two-thirds agree their IT security budget is sufficient. Cloud security spending surpassed the amount spent on physical security (from the total IT budget).
- Cloud security spending increased for 48 percent of the companies in the past year, while the IT security budget for other security activities remained the same.
- Only 64 percent of cyberattacks can be stopped, detected or prevented with the current resources.
- Some 34 percent of companies were breached in the past 12 months, while 74 percent of IT decision makers don't know how the company was breached.
- Two-thirds of companies would pay an average of \$124k to avoid public shaming scandals after a breach. Some 14 percent would pay more than \$500k.



**2016 gave rise to** unknown security challenges that IT decision makers have to prevent by adopting breakthrough technologies able to fight zero-day exploits, Advanced Persistent Threats, and other devastating types of cybercrime. Furthermore, virtualization and adoption of hybrid environments have significantly increased the attack surface, causing more headaches for those who have to secure all infrastructures, physical or not. More businesses are entrusting more sensitive data and workloads to cloud providers, as 63 percent of companies already run IT operations in the cloud, 36 percent operations, 34 percent customer service, marketing and sales, and 32 percent finance too<sup>1</sup>.

The hybrid cloud market will grow at a compound annual rate of 27% until 2019, according to research firm MarketsandMarkets, as

<sup>1</sup> "Moving forward with cybersecurity and privacy", PwC, Oct 2016, <http://www.pwc.com/gx/en/information-security-survey/assets/gsis-report-cybersecurity-privacy-safeguards.pdf>



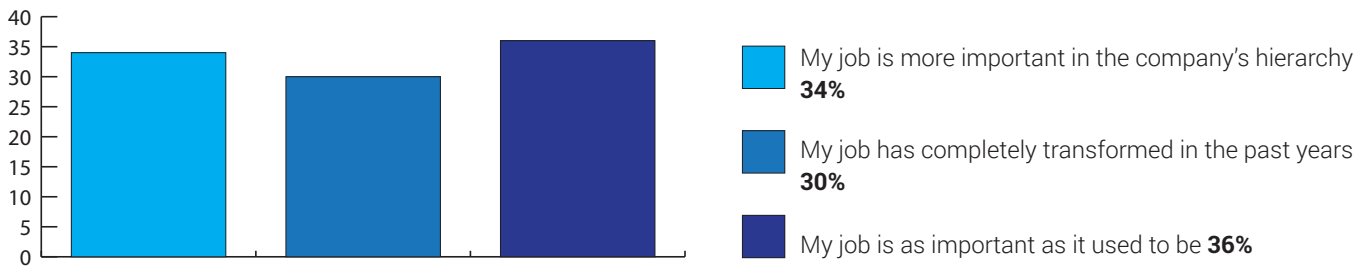
cited by The Journal<sup>2</sup>. The company expects the hybrid cloud market to more than triple to \$85 billion in 2019, from \$25 billion in 2014. Gartner surveyed attendees at one of its tech conferences and found that nearly 75% of large enterprises there planned to have hybrid IT deployments, as in the hybrid cloud, by the end of last year. Large companies that have invested heavily in on-premise architectures and migrated data to the cloud will be the biggest ambassadors of the hybrid model.

These changes occur in a brutal reality where cybercrime led to estimated financial losses of more than \$500 billion in 2015 alone, - and that may be doubling in 2016. From ransomware attacks aimed at a quick buck, to APTs (Advanced Persistent Threats) aimed at siphoning intellectual property and customer data, cybercrime has also become a highly profitable industry. Many of these complex attacks have been successful, realizing [Bitdefender's predictions about the complex threat landscape](#) in 2016.

*“On the business side we will see an increase of targeted attacks and strongly obfuscated bots, with a short lifespan and frequent updates. Most of these attacks will specialize in information theft,” Bogdan Dumitru, Bitdefender’s Chief Technology Officer, predicted in December 2015. “Attackers will be in and out of an organisation in a few days, maybe even hours. APT, which currently stands for Advanced Persistent Threats, should change to BA for Blitzkrieg Attacks,” he said. “Lateral movement in the infrastructure of cloud service providers will increase with the advent of tools that allow hackers to compromise the hypervisor from a virtual instance and jump to a different virtual machine. This scenario is particularly dangerous in ‘bad neighbourhood’ environments where an ill-intended party could get to share a physical system with a legitimate service provider or business.”*

A Bitdefender study on large US companies revealed that *the rising pressure of cyber breaches and Blitzkrieg Attacks has prompted* CEOs to consider CIOs as one of the most important C- level managers, joining COOs and CFOs in decision-making strategies, and bringing security to board-level thinking. Some 34 percent of IT decision makers feel their job is more important in the company organigram than ever before, while another 30 percent admit their job has completely changed in the past years.

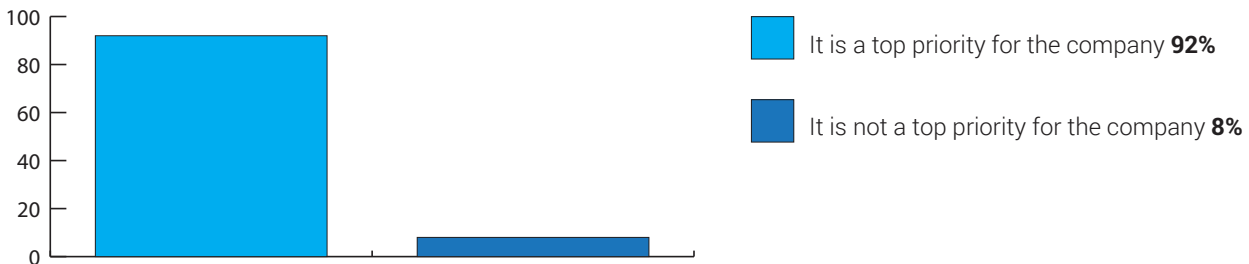
**Hybrid environments brought the CIOs in the boardroom (%)**



Even though nine in 10 IT decision makers perceive IT security as a top priority for their companies, they think the budgets need to increase by 34% to deliver efficient IT security policies.

According to Gartner, the lack of engagement with the business is a major cause of differing risk views between the security team and the business, which can result in redundant and mismanaged controls, which in turn result in unnecessary audit findings and ultimately in reduced productivity<sup>3</sup>.

**Perception on the IT security budget (%)**



Bitdefender’s survey shows that 64 percent of IT decision makers think that the IT security budget is sufficient, 26 percent say the budget is sufficient but they are understaffed, and 7 percent say it is sufficient but could not accommodate future expansion. Only 3 percent of IT decision makers surveyed said the IT security budget in their company is insufficient.

<sup>2</sup> SPECIAL REPORT: CIOs Say Hybrid Cloud Takes Off, WSJ, <http://blogs.wsj.com/cio/2015/10/20/special-report-cios-say-hybrid-cloud-takes-off/>

<sup>3</sup> “Gartner Survey Shows Information Security Governance Practices Are Maturing”, Gartner, July 21, 2015, <http://www.gartner.com/newsroom/id/3098118>

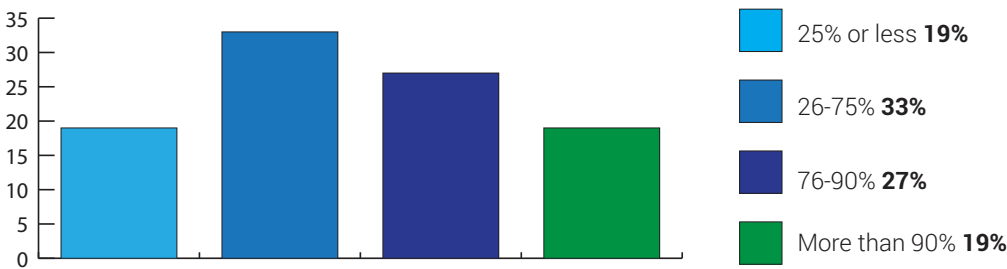




Security's arrival at board level is also confirmed by one in three CEOs, who admit having met four to six times in the past 12 months with their executive team or board of directors on cyber security. Changes will continue to happen as IT security budgets increase in coming months and more chief information security officers believe hackers may gain the upper hand two to five years from now, requiring stronger and more innovative defensive measures. And CEOs have started to understand that, although CIOs are not certain of all the methods malicious hackers use to infiltrate systems, and businesses do not want to disclose their safety measures, as previous studies confirmed<sup>4</sup>.

Cloud security spending increased for 48 percent of the companies in the past year, while the IT security budget for other security activities remained the same, Bitdefender's survey shows. While almost two-thirds of IT decision makers say the security budget is sufficient, the rest would need a future increase of 34 percent, on average, to deliver efficient IT security policies. This is mainly because migrating information from traditional data centers to a cloud infrastructure has significantly increased companies' attackable surface, bringing new threats and more worries to CIO offices regarding the safety of their data. From the total base of the IT decision makers, they say only 64 percent of cyberattacks can be stopped, detected or prevented with the current resources, on average.

**IT security attacks that can be stopped/detected/prevented with the current resources (%)**

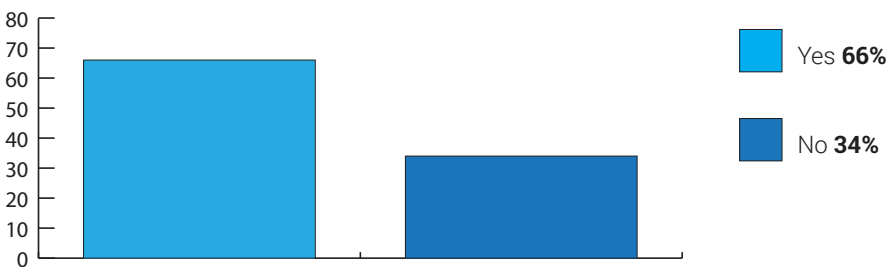


Bitdefender's survey shows 34 percent of companies were breached in the past 12 months, while 74 percent of IT decision makers don't know how the company was breached.

Cybercriminals can spend large amounts of time inside organizations without being detected - APTs are often defined as designed to evade detection. In the virtualization paradigm, since nothing being executed in raw memory is encrypted – just scrambled – APTs that try to execute malicious code on a virtual machine will be intercepted by Bitdefender's Hypervisor Introspection technology long before they actually compromise the operating system. In fact, as soon as the malicious code, even delivered via zero-day exploit, tries to execute in the VM's memory, the introspection engine will immediately "see" the malicious action and the code that was trying to execute.

Moreover, two thirds of companies would pay an average of \$124k to avoid public shaming scandals following a security breach. Some 14 percent would pay more than \$500k, confirming that negative media headlines could have substantial financial consequences. In a recent case, officials from Verizon, which agreed to buy Yahoo's core properties for \$4.83 billion in July, told reporters that the company has "a reasonable basis" to suspect that the Yahoo security breach, one of the largest ever, could have a meaningful financial impact on the deal, according to multiple reports. This further highlighted the risk that cyber incidents could eventually destroy significant transactions or even whole under the enormous pressure from both stakeholders and media. In the minds of board members, IT decision makers in C-level suites deserve the blame for breaches. Failure to mitigate and act quickly and efficiently in case of a breach can cost CIOs and IT manager their jobs.

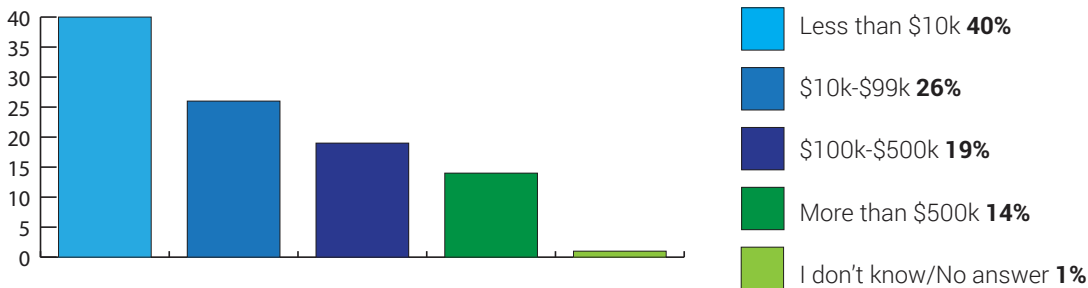
**Payment for avoiding a security breach (%)**



4 "The Defender's Dilemma Charting a Course Toward Cybersecurity", [http://www.rand.org/pubs/research\\_reports/RR1024.html](http://www.rand.org/pubs/research_reports/RR1024.html)



**The amount the company would pay (%)**



With all this in mind, organizations that have, or plan to adopt, a hybrid cloud should consider a couple of practices to make sure their data and their customers’ data is always secure.

**1. Define the criteria on which you store on-premise or in-the-cloud data. Perform risk management.**

Security specialists advise that, when opting for a hybrid cloud solution, an organization must first analyze the type of data it’s handling and evaluate it based on its level of sensitivity – both for the company and its clients. Critical, personal and private data related to intellectual property must be stored on premise, with access to it available only to authorized personnel.

**2. Keep your cloud private.**

Organizations that handle sensitive or confidential data, or data related to intellectual property, need to ensure their private cloud infrastructure remains private. No one outside the local network should be able to access that data and only authorized personnel should be vetted for handling it. The private cloud needs to be completely isolated from public internet access to prevent attackers from remotely accessing the data due to security vulnerabilities.

**3. Be mindful of geographical jurisdiction and data handling storing laws**

When choosing a cloud service provider, it’s vital that the datacenter physically reside in a region or country in which data handling and storing legislation is favorable to your company’s business interests. Any datacenter, regardless of the data it stores, falls under the data



privacy and protection laws of the country it's built in. Consequently, it's vital that any company that plans to use a cloud service provider that has datacenters outside its borders read and abide by the local [data protection laws](#). Otherwise, the organization may risk judicial repercussions that could involve both financial and reputational damages.

4. **Perform due diligence on the cloud service provider and stipulate damages.**

When choosing a cloud service provider, it's imperative that a due diligence report be executed to assess both the provider's capacity to serve the client's needs and his ability to recover in case of technical accidents (e.g. power outages, data corruptions, hardware failures) and natural causes (e.g. earthquakes, fire hazards). This guarantees business continuity for your organization, and helps draft and enforce emergency procedures that need to be set in place as soon as such accidents occur.

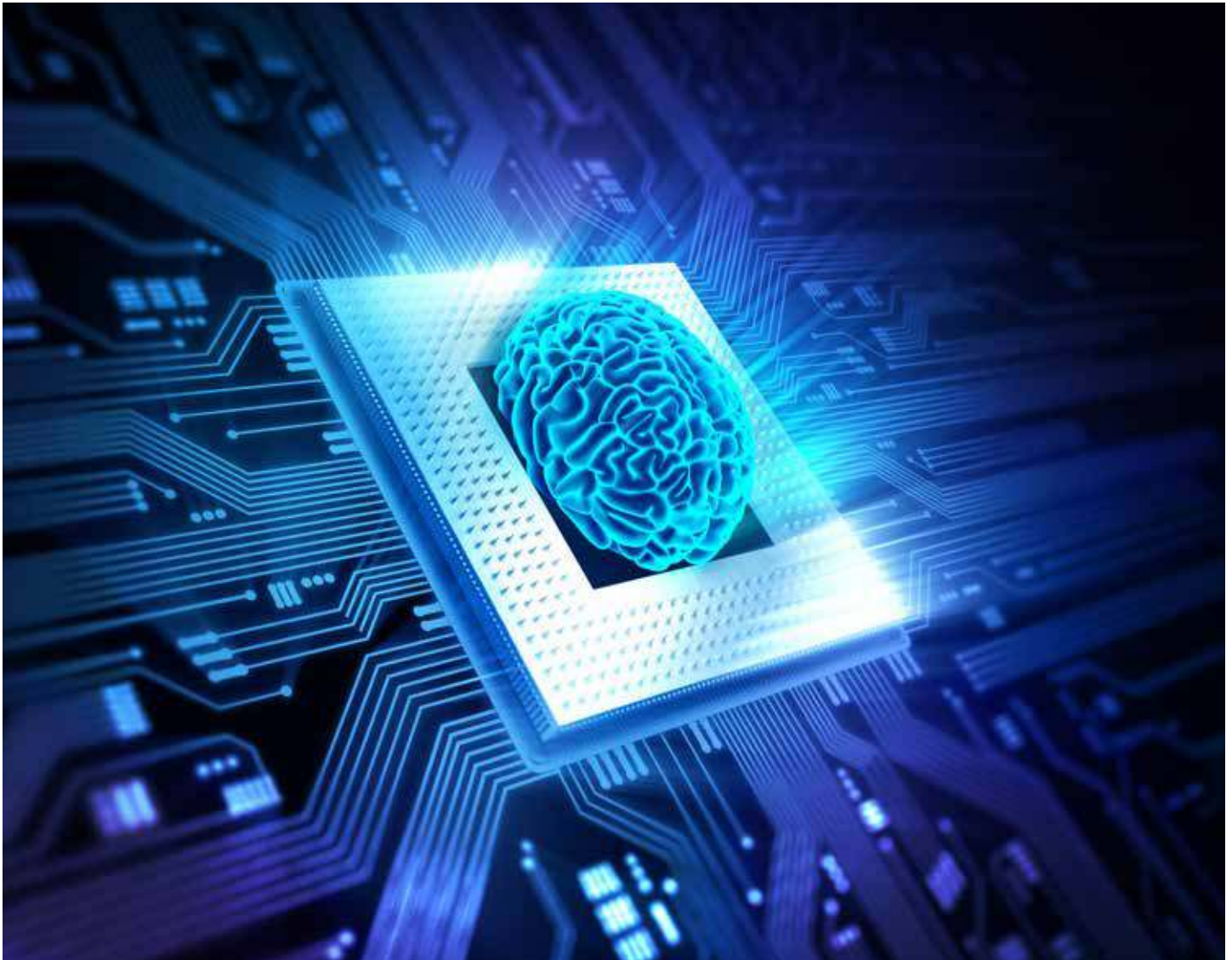
5. **Encrypt data both locally and in transit**

Bitdefender security specialists recommend that any data transfer between the client and the cloud service provider needs to be encrypted to avoid man-in-the-middle attacks that could intercept and decipher all broadcasted data. Beyond that, any data stored locally or in the cloud should be encrypted to make sure cybercriminals cannot read it, in case of data breaches or unauthorized access.

6. **Backup cloud data**

To guarantee business continuity, organizations should have backup and recovery mechanisms – preferably in remote physical or virtual locations, different from your current cloud service provider – to minimize damages from errors or natural disasters.

7. **Use secure and multiple authentication mechanisms**





Accessing any type of data, whether in the private or public cloud, needs to be done via multiple authentication mechanisms, Bitdefender's security specialists recommend. These should involve a lot more than just usernames and passwords. For access to critical data, two-factor or even biometric data could offer additional control and authorization of qualified and accepted personnel.

8. **Limited number of employees that can access sensitive data**

Only authorized personnel needs access to critical and sensitive data, and only by adhering to strict security protocols and advanced authentication mechanisms. Besides two-factor authentication, even two-person authentication could be set in place for critical systems, similar to financial institutions where large transactions must be authorized by two or more individuals.

9. **Prevent DDoS attacks**

Distributed Denial of Service (DDoS) attacks can limit or sometimes even completely disrupt cloud services. Consequently, organizations need to implement systems that can automatically manage and handle DDoS attacks to ensure business continuity even when under fire from such attacks. [Constantly monitoring network traffic](#) to identify anomalies and inconsistencies is also considered good practice.

10. **Create, define and implement fast security response procedures**

Companies need to define a set of procedures and rules to handle security incidents, which all stakeholders must abide by. These must cover techniques and methods for identifying, isolating and remedying security breaches. After any security incident, it's mandatory to evaluate its impact on both the company and its infrastructure, as well as apply the new and necessary security mechanisms for preventing those types of breaches or vulnerabilities.

## Methodology

This survey was conducted in October 2016 by iSense Solutions for Bitdefender on 250 IT security purchase professionals (CIOs/CEOs/CISOs – 26 percent, IT managers/directors – 56 percent, IT system administrators – 10 percent, IT support specialists – 5 percent, and others), from enterprises with 1,000+ PCs based in the United States of America.

More than half of the organizations surveyed are from the IT hardware and software / electronic and electrical engineering industries, while 24 percent are from manufacturing, 6 percent from transportation, 4 percent are providers of telecommunication services, 4 percent are utility or public services companies, and the rest come from construction, retail, distribution, media or other industries.

Some 62 percent of the organizations surveyed have over 3,000 employees, 14 percent between 2,000 and 2,999, and 24 percent between 1,000 and 1,999.

Regarding IT infrastructure development in the organizations, 39 percent of the companies have 3,000+ computers, 21 percent between 2,000 and 2,999, and 40 percent between 1,000 and 1,999. The average proportion of employees working on computers in the organizations surveyed is 74 percent.

Geographically, a third of the organizations are in the West, 30 percent in the North-East, 28 percent in the South and 11 percent in the Mid-West.

Author: Răzvan Mureșan

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at <http://www.bitdefender.com/>.

All Rights Reserved. © 2015 Bitdefender. All trademarks, trade names, and products referenced herein are property of their respective owners.  
FOR MORE INFORMATION VISIT: [enterprise.bitdefender.com](http://enterprise.bitdefender.com)

