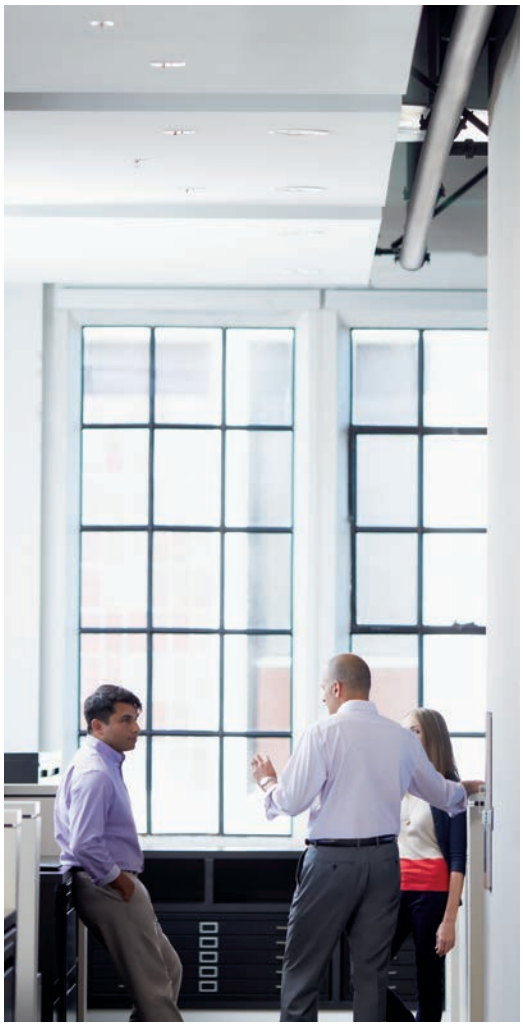
5 Questions Executives Should Be Asking Their Security Teams

Office

Microsoft



Data breaches are more than a security problem. A significant attack can shake your customer base, partner relations, executive staff, profits, and revenue. Historic data breaches have cost executives their jobs, resulted in major revenue losses and damaged brand reputations. In a 2014 study of 700 consumers about brand reputation by Experian and the Ponemon Institute, data breaches were reported as the most damaging occurrence to brand reputation, exceeding environmental disasters and poor customer service.[1] In a world where data breaches have become commonplace, what steps can be taken to minimize damage?

There were 781 reported breaches in 2015, on par with 2014's 783 reported breaches.[2]

[1] Experian: Aftermath of a Mega Data Breach
[2] ID Theft Center's 2015 Data Breach Report

The average consolidated total cost of a data breach in 2015 was $3.8 million—a 23% increase since 2013.

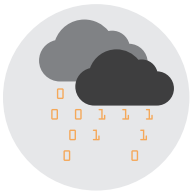
IBM 2015 Cost of Data Breach Study

Security breaches affect your entire organization, and that means leadership must join forces with CSOs in the fight for enterprise security.

Although Chief Security Officers, Chief Information Security Officers, and security analysts are on the front lines fighting hackers, they should not be considered the last and only line of defense. CFOs, typically responsible for managing a corporation's financial risks, should be inquiring on the enterprise risk of cybersecurity. And while other executive roles don't have security measures in their purview, they can take action to help improve their organizations' overall security.

- CTOs may counsel CSOs and CISOs on security software implemented at their organizations but should also focus on the security features of every piece of technology implemented.
- CMOs and marketing executives responsible for their companies' public reputations must be wary of the reputation risks that can result from a breach, developing a publicity plan in the face of an attack in order to protect sales revenue down the line.
- HR and talent management should be aware of what an internal information data breach could do to employee trust, focusing on protection of the confidential information they manage.
- CEOs and board members must recognize the implications faulty cybersecurity can have on their companies' valuation and prioritize security in their company's roadmap.

When it comes to protecting the organizational assets that matter most, what questions should all leadership ask of their security teams?



QUESTION 1

How often do you see non-sanctioned cloud services in use?

Dropbox. Google Drive. MediaFire. Egnyte. Your organization might not support them, but chances are your security team has seen one or more of these private clouds in use within an organization.

"Rogue clouds" (private file sync-and-share options not supported or secured by an enterprise's IT infrastructure) are creeping into organizations. A 2013 survey by Symantec found that 77% of all businesses experienced rogue cloud situations.[3]

To eliminate rogue clouds, security teams should talk with their CTOs about which organizationally sanctioned cloud service is recommended. From there, other members of leadership can weigh in on which solution will be most useful to their employees and business partners. Talk with security teams about implementing organizationally supported cloud solutions. Enterprise-level solutions, like Microsoft OneDrive for Business, enable employees to save, share, and collaborate on documents without compromising data security.

40% of organizations that experienced rogue cloud situations saw confidential data exposed.[3]

[3] Symantec study: Avoiding the Hidden Costs of the Cloud

"The fact that Office 365 is backed by Microsoft is huge. I'll never have to change providers again because I trust Microsoft to look after our email and other services for us."

Paraic Nolan
Finance Director
Big Red Book

QUESTION 2

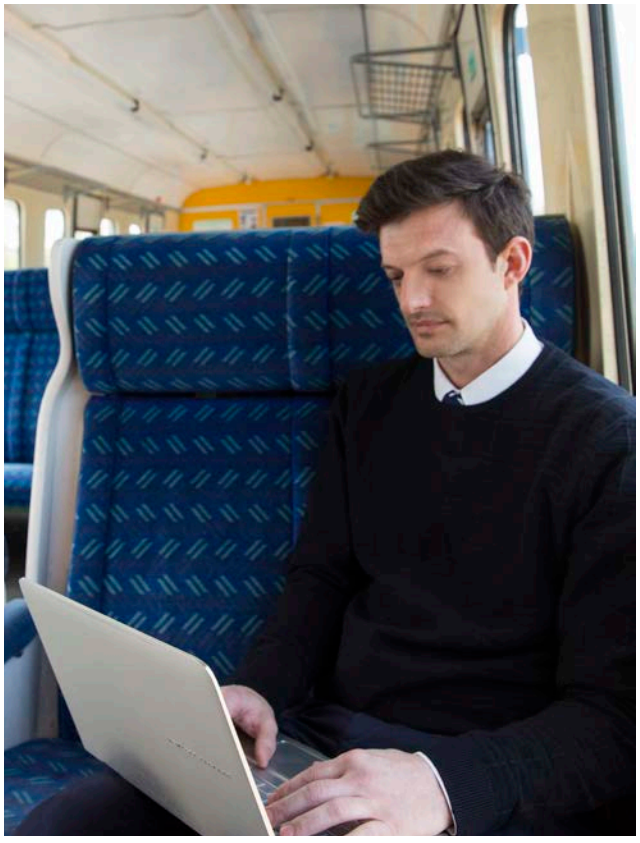
Are we protecting ourselves against insider threats?

Insider threats are commonly thought of as one of the most difficult threats to defend against. With the growing use of contractors, freelancers, and temporary employees throughout an enterprise, defending against potential internal threats seems next to impossible. In 2013, the FBI estimated malicious insider threat attacks cost approximately $412,000 per incident.[4]

Although there is no single solution for defending against insider threats, experts recommend a multi-pronged approach that involves action from several members of leadership. Talent acquisition should focus on strong background checks on all employees and contractors, and human relations can help catch red flags stemming from irregular employee behavior (such as missed work or bragging about potential damage they could do).[5] CFOs and CTOs can discuss the possibility of implementing security behavioral monitoring tools to identify instances when any employees access files they have no relation to, files or information is saved to an external location, or employee logins happen at irregular times.

Fortunately, if suspicion of internal threats does arise, solutions like Microsoft Data Loss Prevention (DLP) rolled into OneDrive for Business, SharePoint Online, Exchange, and Office 2016, will enable your IT administrators to protect against data loss without stretching their compliance budgets.

Administrators will receive notifications if confidential information is being exchanged, and they have the opportunity to recall data and access from certain employees. Additionally, with DLP, administrators can review incident data and generate incident reports to see exactly where information may have been leaked.



[4] Fred Donovan, FierceITSecurity: Is the person sitting next to you a malicious insider?
[5] George Silowash, Software Engineering Institute: Common Sense Guide to Mitigating Insider Threats: 4th Edition

You don't just need to defend against viruses and malware—19% of security incidents involve malicious insiders.

Fred Donovan, FierceITSecurity: Is the person sitting next to you a malicious insider?

QUESTION 3

Do we have a cybersecurity task force in place?

Cybersecurity professionals are taught to think of when (not if) a breach will occur. Planning for a breach means creating a task force across an organization that designates who will be involved in disclosing the attack to customers (the CMO), who will be responsible for securing a network (the CISO, CSO, and CTO), and who will handle legal ramifications of the breached information (legal, customer, and HR departmental leads). Although creating a cybersecurity task force within an organization is considered a best practice, most organizations don't have a task force in place at all.

According to a Microsoft Information Security survey, 63% of financial executives of enterprise-level companies believe they are "just keeping up with security threats," 28% believe they are ahead of these threats, and 9% feel they are lagging behind.[6]

Who should be involved? A large portion of the task force will include security analysts and the IT department. But don't overlook the importance of legal, finance, investor, and public relations support. Anyone who would contribute to a breach cleanup should be included on a cybersecurity task force and be ready to take action.

[6] Microsoft Information Security Survey, September–October 2015

84% of organizations have not implemented a cybersecurity task force.

Financial Executives Research Foundation: The CFO's Role in Cybersecurity

QUESTION 4

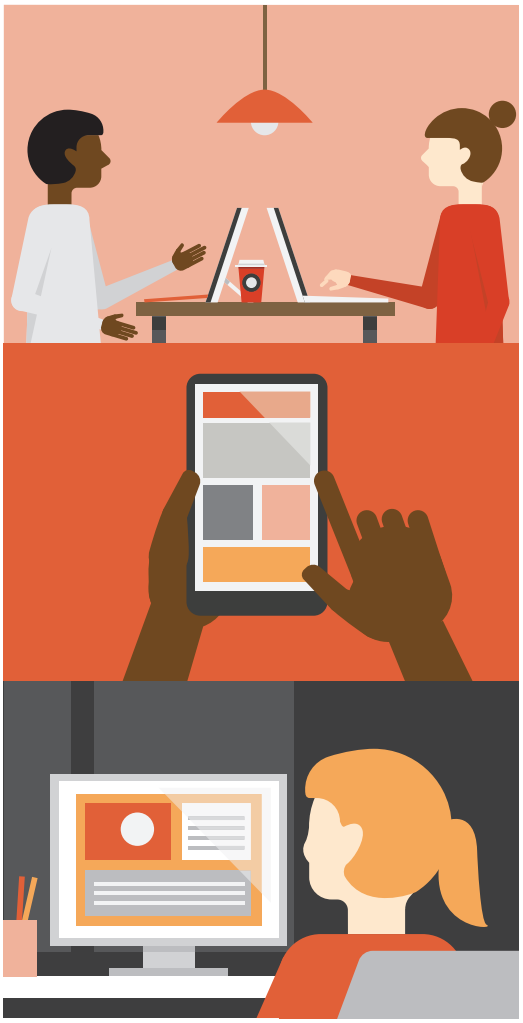
Is our BYOD policy secure?

BYOD policies have exploded in the past five years, enabling employees to access company files on their own devices around the clock. According to a 2014 report by Check Point, however, more than half of IT executives reported that BYOD security incidents cost their organizations more than $250,000 in a two-year period.[7]

It is possible to continue to support BYOD policies without compromising security or breaking your budget. Ask security teams about current offerings' single sign-on capabilities and self-service password management. Mobility management tools like Microsoft Enterprise Mobility Suite can keep employees connected to the apps they need, without compromising security. In a Microsoft Office 365 economic impact report by Forrester, 28% of enterprise users reported seeing an improvement in mobile data security, due to Enterprise Mobility Suite's ability to remote-wipe data from lost devices.[8]

[7] Infosecurity Magazine: BYOD Security Incident Costs Exceed $250,000

[8] Forrester report: The Total Economic Impact™ of Microsoft Office 365, October 2014



Additionally, Office 365 Mobile Device Management (MDM) can help secure your businesses devices from anywhere. Your IT team can manage mobile device policies, and perform a selective wipe of Office 365 data if an employee leaves your organization, saving your HR, IT, and security departments time and headaches.

"We needed to secure and manage the mobile devices and smartphones used outside the corporate network—as well as the data they contain. The Enterprise Mobility Suite delivers these capabilities in one, cost-effective package."

Kris Mampaey
Director of IT
Willemen Groep

QUESTION 5

Do you feel limited by your security budget or staff size?

Enterprise security leads are tasked with hiring around-the-clock teams that must manage multiple security solutions and thousands of alerts each day. Are their budgets and hiring allowances within reason? When reviewing the durability of an enterprise's security, leadership must make sure a generous budget is allocated toward rapid security development and evaluate whether any other budgets can shrink to meet these needs.

Be it hiring management assistance, additional analysts brought on staff, or a boost in IT budget—find out what your security team needs, and make the changes necessary to ensure they can best do their jobs.

Cybersecurity spending isn't slowing down. Gartner reported that cybersecurity spending reached a record $75 billion in 2015 and anticipates it reaching $170 billion by 2020.[9]

[9] Steve Morgan, Forbes :Cybersecurity Market Reaches $75 Billion In 2015; Expected to Reach $170 Billion by 2020

Fortunately, many of the tools your company already uses can supplement your security plan. Enterprise-supported file sync and share solutions like Microsoft SharePoint and OneDrive for Business can eliminate employees' use of rogue clouds, while significantly improving the security behind files shared with partners and contractors. Assembling and communicating with a cybersecurity task force can be made easier with office communication tools like Skype for Business web conferencing and Exchange Online. Improve the security of your BYOD policy with mobile apps available for a variety of Office programs across Apple, Android, and Windows devices. Most importantly, all of these tools are available within your budget and likely familiar to your employees through Office 365.

It's time to talk with your security team.

Have we managed our rogue cloud usage? ☐

Have we secured our BYOD policy? ☐

What are we doing to protect against insider threats? ☐

Does my security team have a sufficient budget? ☐

Have we built our cybersecurity task force? ☐

Want more business tips?

Dive inside the minds of business and technology innovators with Microsoft's Modern Workplace webcast series:

https://www.modernworkplace.com/

Office

Microsoft