SOHA

Third Party Access Is A Major Source Of Data Breaches, Yet Not An IT Priority

We have known for years that third parties are the main gateway for data breaches. In a recent Ponemon Institute report (May 2016), 75% of the IT and security professionals surveyed said the risk of a breach from a third party is ***serious*** and is ***increasing***.

But a recent survey by Soha System's Third Party Advisory Group of nationwide Enterprise IT and Security Managers, Directors, and C-Level Executives reveals that ***less than 2% consider third party access a top priority*** despite growing security threats.

Table of Contents

Methodology + Demographics

Soha System’s Third Party Advisory Group conducted an online survey in April 2016 of over 219 IT and Security C-Level Executives, Directors and Managers from enterprise-level companies. The goal was to understand the role and importance of third party access. Respondents represented 22 industry categories. Both small and large organizations completed the survey, with 35% stating there were 10,000+ employees in their organization. Seventeen questions were asked that required single and/or multiple-choice answers. All responses were anonymous.

Why is Third Party Access Not an IT Priority

We have become numb to the constant reports of data breaches at private sector, government and nonprofit organizations. The volume of personal and financial data compromised in recent years is mind-boggling. With 63% of all data breaches linked directly or indirectly to third party access, those contractors and suppliers who need to get access to corporate applications in order to get their job done represent risk to any organization.

While a significant risk vector, only 2% of respondents consider third party access their top IT priority. The survey revealed that nearly every other category of IT spend - ranging from infrastructure to mobile to security - garnered more budget.

And the problem is not going away; in fact it is getting worse. 87% of IT professionals report their organization's use of contractors has increased 49% since 2013, and 40% expect it to increase even more during the next 3 years.

"The results of our survey highlight the disconnect between IT priorities and the urgent need to mitigate third party data breaches," said Mark Carrizosa, chairman of the Third Party Advisory Group and chief information security officer and vice president of security at Soha Systems.

Key Finding:

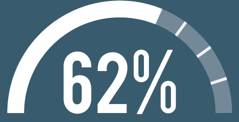
Enterprises have vastly under-resourced third party access, even though it represents a major risk trajectory to their organization.

Breaches Happen, Just Not to Our Company

Even with all of the recent third party breach activity involving such notable brand names as CVS, Samsung, American Express and Experian, the survey reveals IT executives continue to believe that security breaches are something that happens to competitors' organizations, not theirs.

While 62 percent of respondents do not expect their organization to be the target of a serious data breach due to third party access, 79 percent expect their competitors will suffer a serious data breach in the future. And while the respondents didn't believe their organization was vulnerable to an attack through third parties, 56 percent had strong concerns about their ability to control and/or secure their own third party access.

Expect More Breaches



While 62% of respondents didn't believe their organization was vulnerable to an attack from third parties, ***79% expect their competitors have or will suffer a serious data breach in the future.***

Key Finding: ***IT organizations are increasingly providing third parties with access to their application infrastructure, but IT and security leaders need to help their business leaders understand the risks of third-party access.***

Granting Third Party Access is Complex

"The complexity of providing secure access to applications spread across many cloud instances or in multiple data centers, to contractors and suppliers who do not work for you, using devices you know nothing about, is a really hard problem," said Haseeb Budhani, CEO and co-founder of Soha Systems. "It takes a long time to work through the moving parts".

75 percent of survey respondents agree they have to touch numerous network and application components when adding new, external user groups (on average, between 5 and 14 different hardwares and softwares).

55 percent of respondents said providing third party access to new supply chain partners was a "Complex IT Project", and 57 percent agree that "it is a pain to enable, deploy, and manage."

Key Finding:
Third party access has lots of moving parts, and is painful to manage and sustain.

Lots of Moving Parts

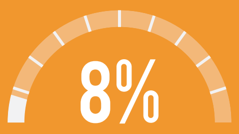
agree they have to touch ***5 to 14 network and application components*** when adding new external user groups.

Third Party Data Breaches Do Not Equate to IT Job Loss

"While a few high profile data breaches have resulted in C-level firings, for the most part, IT professional are not concerned about losing their job should a breach occur," said Carrizosa. "But there is a substantial sense of professionalism and personal pride for those in a role where their actions could prevent a breach."

The survey asked IT execs, "If a data breach occurred in your area of responsibility, would you feel personally responsible?" Interestingly, 53 percent of respondents said they would feel personally responsible if a data breach occurred in their area because they felt it would reflect poorly on their job performance, but only 8 percent thought they might lose their job if a data breach occurred during their watch. IT takes their jobs seriously but it is unclear who is being held accountable for data breaches and how this ambiguity might affect attitudes and behavior in ensuring organizations are safe from outside threats.

Who's Accountable?



But only 8% thought they ***might lose their job*** if a data breach occurred during their watch.

Key Finding:
IT professionals barley worry about third party risk accountability. While IT managers are concerned about their role in data breaches, most do not believe they will suffer personal consequences if a breach occurs

About Advisory Group Formed to Address the Problem

As the survey data clearly shows, the gap between IT priorities and third party access risk is a serious problem that affects all industry segments. And to help determine why this has been such ongoing problem, Soha formed the Third Party Advisory Group to act as a conduit for ongoing research —including this most recent IT survey — and establish future guides for ongoing best practice recommendations on the topic of third party access.

The Advisory Group features a number of security professionals, analysts and industry influencers including chairman Mark Carrizosa. Mark is Soha's chief information security officer and vice president of security, and joined Soha in 2015 from Walmart where, as principal security architect, he developed and implemented the company's global e-commerce security architecture framework. Prior to Walmart, Mark was operational risk consultant at Wells Fargo where he analyzed the company's infrastructure and application compliance to improve the security risk posture of both customer-facing and internal systems.

Additional advisory group members include Derek Brink, vice president and research fellow at Aberdeen Group; Andy Champagne, vice president and chief technology officer (CTO) at Akamai Labs; Steve Hunt, principal consultant at Hunt Business Intelligence; Slava Kavsan, founder and chief executive officer (CEO) at CKure Consulting; Mike Kotnour, senior information security advisor at Assurant Solutions; Shahed Latif, principal in the cybersecurity and privacy practice at PwC; Ajay Nigam, senior vice president products at BrightPoint Security; and Nico Popp, senior vice president, information protection at Symantec; and James Rutt, Chief Technology Officer at the Dana Foundation The group's next survey and their recommendations are on the schedule for Fall 2016.

About Soha System

Soha Systems, named a "Cool Vendor" in "Cloud and Emerging Technology Security, 2016" report by Gartner, Inc., is an innovator of enterprise access as a service for third parties, including suppliers, contractors and franchisees. The service, Soha Cloud, provides a convenient, secure and centralized controlled approach to third party access that does not require device specific software or direct access to the network. The Soha Cloud service, compliant with PCI DSS 3.1, can be deployed in minutes for third party access to corporate applications in data centers and hybrid cloud environments.

For more information,
visit ***http://www.soha.io*** and join the conversation on Twitter
@SohaSystems.