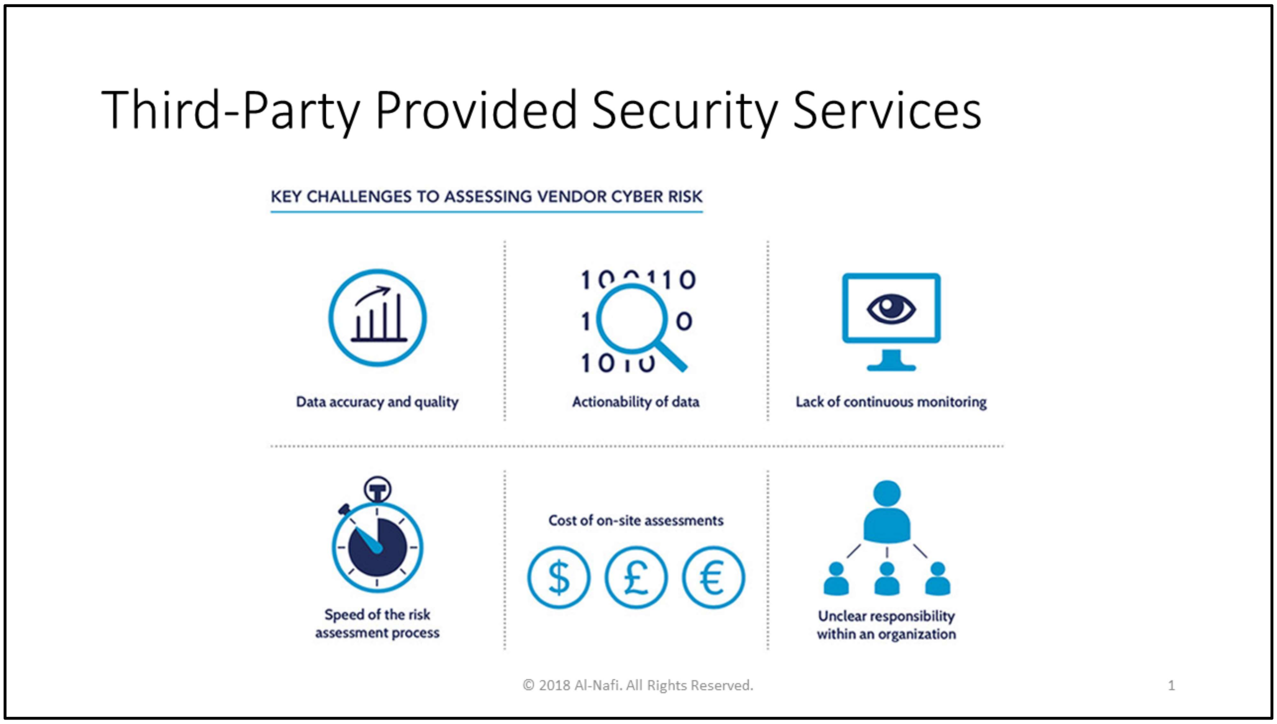


Third-Party Provided Security Services

KEY CHALLENGES TO ASSESSING VENDOR CYBER RISK

Data accuracy and quality

Actionability of data

Lack of continuous monitoring

Speed of the risk assessment process

Cost of on-site assessments

Unclear responsibility within an organization

Managing third-party cyber risk is critical for businesses, but a lack of continuous monitoring, consistent reporting, and other blind spots are creating challenges that could leave organizations vulnerable to data breaches and other consequences.

Most organizations work with hundreds, if not thousands, of third parties, creating new risks that must be actively managed.

The financial industry, in particular, has a massive business ecosystem made up of legal organizations, accounting and human resources firms, management consulting and outsourcing firms, and information technology and software providers.

Each of these vendors poses a potential weak spot for cyber defenses if risk is not actively managed to protect the exchange of data and other sensitive information.

A BitSight and Center for Financial Professionals (CeFPro) joint study “Third-Party Cyber Risk for Financial Services: Blind Spots, Emerging Issues & Best

Practices" sheds light on how financial institutions are addressing challenges associated with third-party cyber risk.

"Managing third-party cyber risk has rapidly become the #1 concern for businesses," said Jake Olcott, Vice President of Communications and Government Affairs at BitSight. "Many in the financial sector are taking action to manage that risk, but as our survey shows, there is vast room for improvement in key areas like continuous monitoring and effective board reporting."

Key findings from the Third-Party Cyber Risk for Financial Services report

Third-party cyber risk is driving key business decisions. Nearly 97 percent of respondents said that cyber risk affecting third parties is a major issue. Meanwhile, nearly 80 percent of respondents said they have terminated or would decline a business relationship due to a vendor's cybersecurity performance. 1 in 10 organizations has a role specifically dedicated to vendor, third-party or supplier risk.

There is a lack of consistent third-party risk measurement and reporting. Only 44 percent of respondents are reporting on this risk to their executives and boards on a regular basis. This lack of regular reporting could be the reason why nearly 1 in 5 respondents think boards and executives are not confident or do not understand their approaches to third-party risk management (TPRM).

A majority of organizations aren't using critical tools. Respondents reported that they still rely on tools like annual on-site assessments, questionnaires and facility tours to assess third-party security posture, giving them limited visibility into their third-party cyber risk. Meanwhile, only 22 percent of organizations are currently using a security ratings service to continuously monitor the cybersecurity performance of third parties, though 30 percent are currently evaluating security ratings providers.

TPRM challenges and concerns for the future continue to grow. Companies are concerned with the accuracy and actionability of risk assessment data, as well as an unclear responsibility for this type of risk management within their organizations. Looking toward the future, respondents are focused on making their security programs more effective while staying up-to-date on new regulations and prioritizing continuous monitoring and visibility.

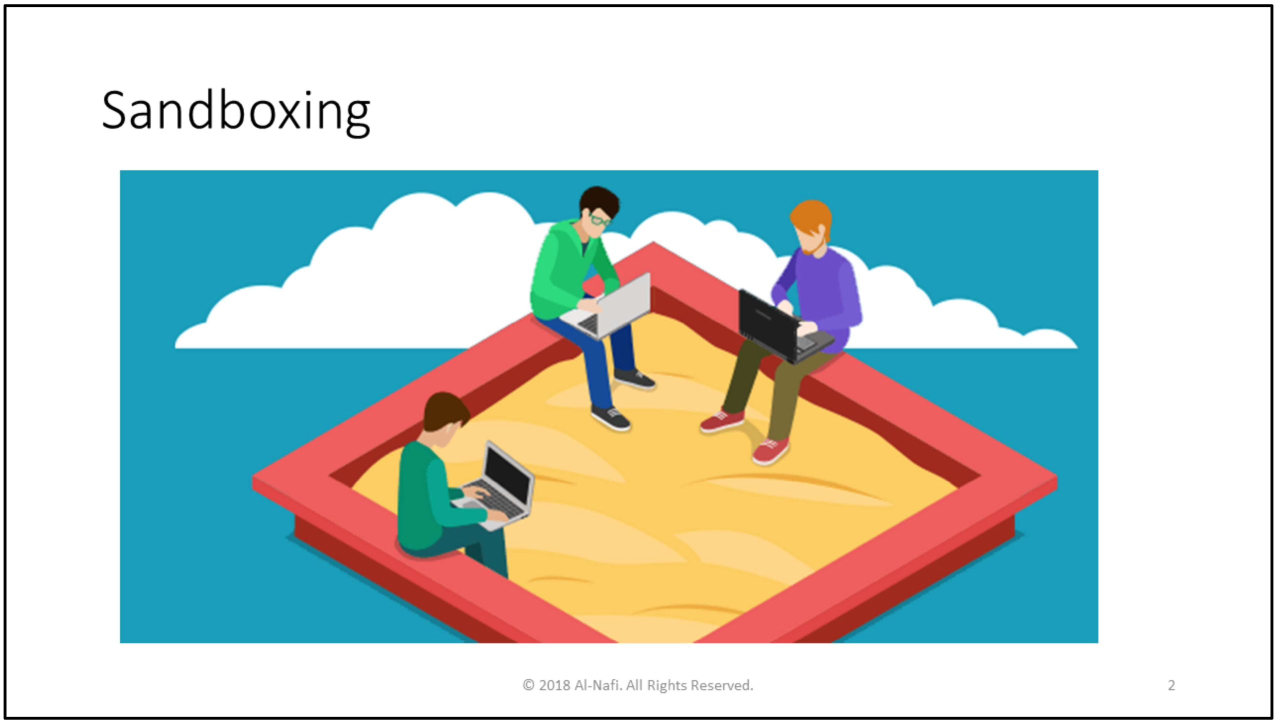
“This report raises a number of interesting questions and challenges for the industry; with C-suite professionals taking responsibility, it is clear that the vast majority of respondents’ organizations understand the critical importance of third-party cyber risk; it is also apparent that there needs to be clarity going forward, with increased communication up to the Board level,” said Andreas Simou, Managing Director at CeFPro.

“Although there has been a significant increase in effectiveness, attention, and resources focused toward third-party cyber risk over the last few years, there is still much to be done; utilizing more effective tools and techniques to overcome the ever-increasing challenges being faced within the industry, with third- (and fourth-) party cyber risk as just one key area to be addressed. The report highlights a number of potential solutions and ways forward.”

New tools and best practices are becoming readily available to help organizations address some of the key challenges and concerns uncovered by the survey.

In order to effectively manage this growing risk and stay ahead of future challenges, organizations must utilize best practices and trust continuous monitoring solutions like security ratings to help measure and manage their cyber risk with third-party risk data that is accurate and actionable.

Reference https://www.helpnetsecurity.com/2019/04/03/third-party-cyber-risk-management-approaches/



Sandboxing

In cybersecurity, a sandbox is an isolated environment on a network that mimics end-user operating environments. Sandboxes are used to safely execute suspicious code without risking harm to the host device or network.

Using a sandbox for **advanced malware detection** provides another layer of protection against new security threats—zero-day (previously unseen) malware and stealthy attacks, in particular. And what happens in the sandbox, stays in the sandbox—avoiding system failures and keeping software vulnerabilities from spreading.

Threats Sandbox Testing Protects Against

Sandbox environments provide a proactive layer of **network security** defense against new and Advanced Persistent Threats (APT). APTs are custom-developed, targeted attacks often aimed at compromising organizations and stealing data. They are designed to evade detection and often fly under the radar of more straightforward detection methods.

How Does Sandbox Technology Work?
Sandbox testing proactively detects malware by executing, or detonating, code in a safe and isolated environment to observe that code's behavior and output activity. Traditional security measures are reactive and based on signature detection—which works by looking for patterns identified in known instances of malware. Because that detects only previously identified threats, sandboxes add another important layer of security. Moreover, even if an initial security defense utilize artificial intelligence or **machine learning** (signature less detection), these defenses are only as good as the models powering these solutions – there is still a need to complement these solution with an advanced malware detection.

Sandbox Security Implementations

There are several options for sandbox implementation that may be more or less appropriate depending on your organization's needs. Three varieties of sandbox implementation include:

Full System Emulation: The sandbox simulates the host machine's physical hardware, including CPU and memory, providing deep visibility into program behavior and impact.

Emulation of Operating Systems: The sandbox emulates the end user's operating system but not the machine hardware.

Virtualization: This approach uses a virtual machine (VM) based sandbox to contain and examine suspicious programs.

Reference https://www.forcepoint.com/cyber-edu/sandbox-security