Simplifying the Problem: Security Planning Through Vendor Management
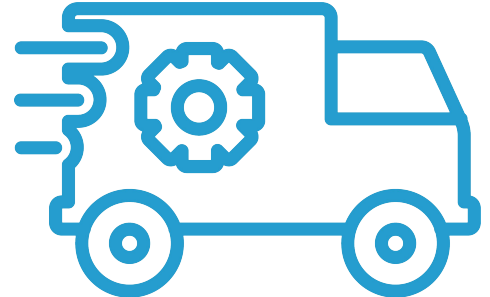
yottabyte

What is Vendor Management?

Vendor Management encompasses the selection and ongoing management of third-party providers of products or services.

Effective Vendor Management requires a proactive approach to setting expectations, roles, and responsibilities between your organization and the vendor organization.

Why is Vendor Management Important?

- Vendors play a key role in the success of your organization and the security of your data.
- Selection of a wrong software package can turn out to be costly and adversely affect business processes.
- There is a lack of confidence in third parties' data safeguards, security policies and procedures.
  - 57% of companies said they cannot determine whether vendor "safeguards and security policies are sufficient to prevent a data breach."
  Ponemon Institute Research; September 2017

Maintain a Consistent Selection Process

Challenge:

- Vendor selection continues to become more complex and burdensome due to the ever-increasing number of products available, incompatible hardware and software configuration, and demanding technical knowledge.

Ferland and Flachbarth, 2018

Solution:

- Develop and maintain a consistent vendor selection process at your organization, so you're always choosing the right vendors for your unique business requirements
- NIST Cybersecurity Framework is a great (and free) resource for building your process

yottabyte

Define Goals
Outline what you're looking for in your new vendor

Pre-Selection
Establish a timeline for selection, assemble team, compile list of possible vendors

Selection
Select vendors to request more information from, write an RFI, evaluate responses to create a "short list"of vendors, select the winning vendor

Contract Initiation
Negotiate and understand the terms of the agreement before signing the contract

Contract Signed

A Deloitte survey of 2,000 consumers in the U.S found that 91% of people consent to legal terms and services conditions without reading them.

Mitigate Risk

Challenge:

- On average, **there are 181 vendors granted network access to a single company each week.***

- Keeping open and honest communication and establishing accountability with each vendor is no simple task.

  *Bomgar Secure Access Threat Report, 2017

Solution:

- Define who your "highest risk" vendors are and prioritize monitoring these most regularly
- Try to work with vendors that can fulfill multiple business needs
  a. Multiple vendors means more exposure to the outside world and more data breach points which could be exploited

yottaby+e

Measure Performance

Summary

- **Develop a consistent process for vendor selection**; the success of your organization and the security of your data depends on the success of your relationships with vendors.

- **Mitigate risk with your chosen vendors**. Communicate constantly and prioritize vendors with the highest risk. Try to choose vendors that fulfill multiple business needs.

- **Measure the performance of your vendors**. Set goals ahead of time, and evaluate whether or not the vendor helped you achieve those set goals.

References

Ferland, Christopher, and Justin Flachbarth. "IR and Vendors: Selecting the Right Product." *New Directions for Institutional Research* 2018.178 (2018): 27-37. *Wiley Online Library*. Web. 18 Apr. 2019.

Jacques, Samantha, and Aimee Watson. "Proactive Vendor Management for Healthcare Technology." *Biomedical Instrumentation & Technology* 51.2 (2017): 116-9. ProQuest. Web. 18 Apr. 2019.

"2017 Global Mobile Consumer Survey" US edition by Deloitte. 2017.

"Data Risk in the Third-Party Ecosystem: Second Annual Study" by Ponemon Institute LLC. September 2017.

"Secure Access Threat Report" by Bomgar. 2017.