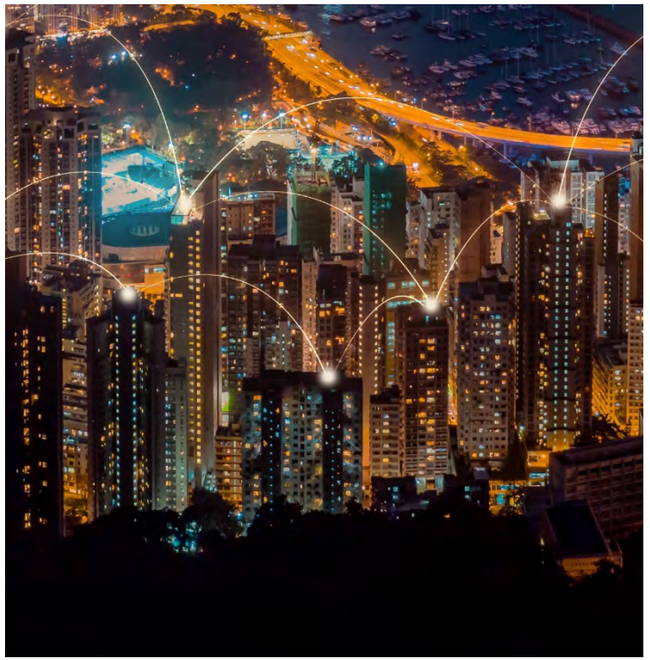
9 STEPS TO MANAGING THIRD-PARTY INFORMATION SECURITY RISK

AVERTIUM

INTRODUCTION

Globalization has had far-reaching implications. Not the least of which is in the area of data sharing between vendors, partners and all other entities in the supply chain. More interconnectivity brings more complexity and greater cyber risks. This in turn demands more robust security measures which can be time-consuming and expensive to achieve.

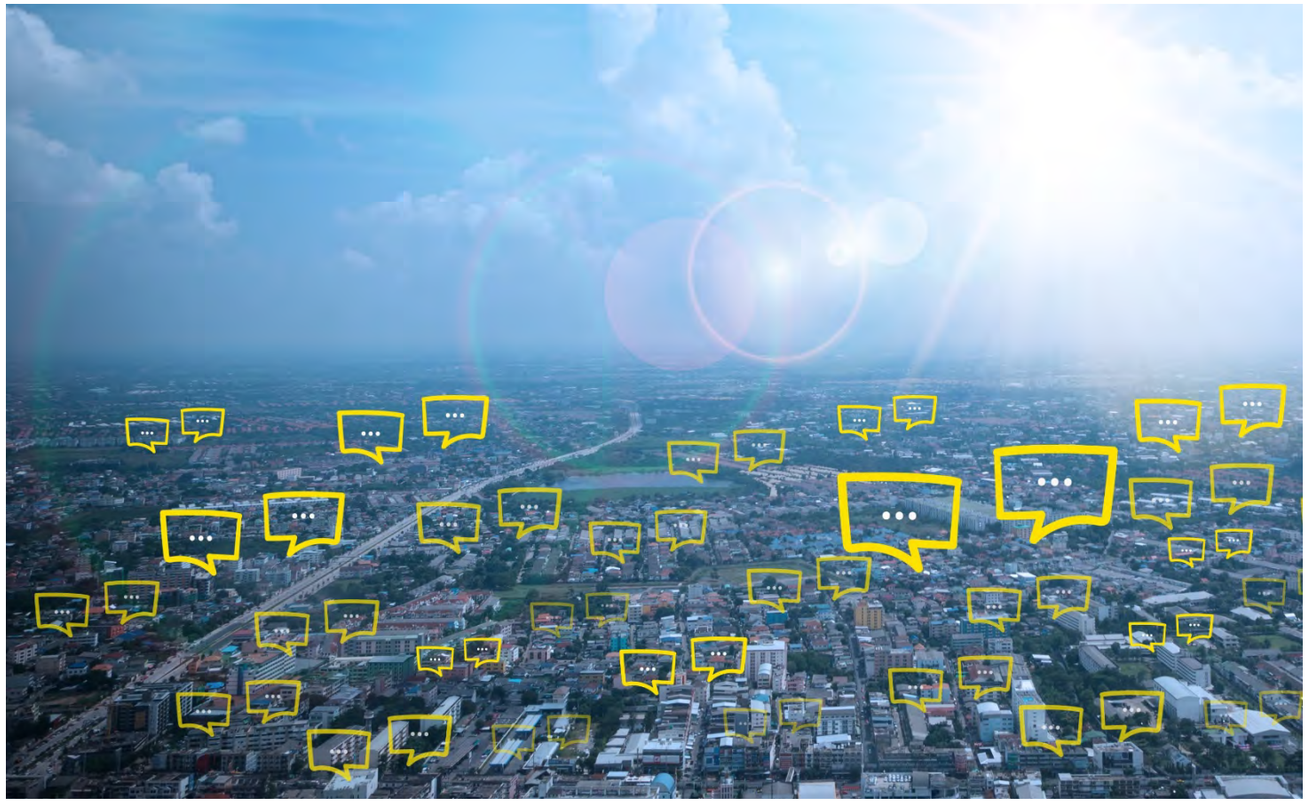
As data breaches resulting from third-party vulnerabilities could cost a company north of seven figures in financial losses, penalties and legal fees, it is not surprising that managing information security risk continues to be a point of focus in third party management programs (TPM).



Once only the concern of regulated banks, TPM programs monitor and manage the ongoing behavior, performance and risk (including information security risk) that each third-party relationship represents to a company.

Today, companies from all sectors deploy TPM programs. In the area of cybersecurity compliance, it is prudent for companies to require that vendors, partners and others in the supply chain adhere to established information security standards.

The following is a checklist for those just starting out or as a primer for those whose TPM program is in progress or under review.



> In third-party data breaches, the personal information held by large companies is compromised through a vendor, business partner or supplier. The consequences of such incidents are considerable: Companies lose consumer confidence and loyalty and can face costly penalties for violating data privacy regulations.
>
> — Yaffa Klugerman, Security Boulevard

PLAN AHEAD

» 01

The terms and conditions established in the contract with your vendor, contractor or suppliers set the tone for your relationship with them. Managing third party infosec risk begins during the vendor vetting process.

- During the evaluation phase, be sure the vendor provides documentation on how they handle and protect sensitive data
- Work with procurement and/or legal to incorporate these into the contractual agreement. Include terms stating that they must agree to share in the responsibility of protecting the security and privacy of your company, employees, and customers

REQUIRE 3rd PARTY POLICIES & CONTROLS

≫02

It is incumbent upon an organization to establish and implement policies to ensure vendor and partner cybersecurity policies and processes meet industry standards. At a minimum, these companies should have defined policies and controls.

Verify that all controls and documentation are compliant and accessible.

STIPULATE SECURITY BEST PRACTICES

» 03

Consider specifying vendors, partners and contractors adopt security best practices such as regular vulnerability scans, an annual penetration test, security assessments and security accreditations.

An understanding of how a vendor is addressing gaps in security will help protect both parties. Establish a vendor management system whereby active monitoring and auditing of vendor performance and security is standardized.

ASSESS 4th PARTY RISK

» 04

Even if vendors, partners and contractors meet security standards, there is one other factor to consider: Their sub-contractors.

- Review and require an updated list of authorized sub-contractors
- Provide third-parties onboarding processes and procedures when they add a new sub-contractor to the list
- Request fourth-party information, certifications and self-assessments as part of maintaining compliance and security within the network relationship

DEFINE 3rd PARTY ACCESS CONTROLS

» 05

Most vendors only need access to very specific areas. Leverage a defined access management policy to limit vendor access using physical or network segmentation.

Clearly defining access to specific systems will better protect your organization.

ESTABLISH API GUIDELINES

>> 06

APIs are widely used to transfer data between systems, apps and networks. They are also used to connect containers and microservices when building and deploying legacy apps.

While your DevOps team may deploy API security best practices, it is incumbent upon you to ensure that partners across the supply chain maintain similar standards.

Developing guidelines on how your API connects to partner applications, how it transports data back to the internet and authentication methods, etc. will go a long way toward protecting your customers' information.

EXTEND SECURITY TRAINING TO 3rd PARTIES

» 07

Companies can significantly reduce their risk of a breach by staying one step ahead of attackers with a formal training program.

Many offer security awareness training as part of the new hire onboarding process. Some provide training to employees on a quarterly basis. But by extending training, especially on new regulations and requirements to partners and vendors, you can ensure everyone is on the same page.

The increased knowledge and competency concerning threats, risks and security options brings you closer to the end goal: A more security-aware culture.

STRENGTHEN YOUR SECURITY

» 08

Strengthening your own security posture will help to enforce strong third-party programs.

Basic Elements

- Risk assessments and consistent internal policies with regular tracking and review of data access
- Regular security audits and network vulnerability identification
- Incidence response plan
- Secure sensitive data

LEVERAGE TECHNOLOGY & AUTOMATION

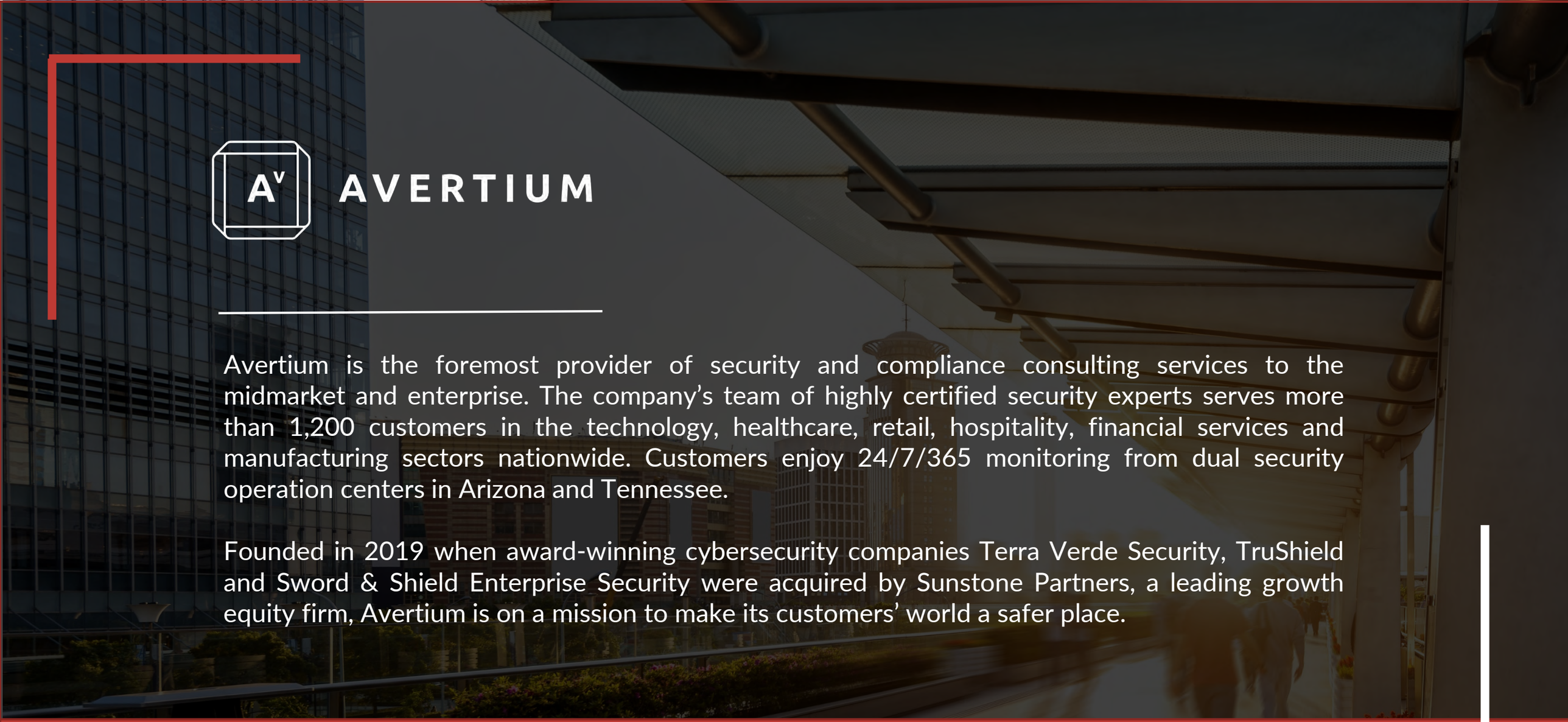
» 09

As third-party management programs continue to expand to include other entities within the security ecosystem, finding the right technology to help streamline, consolidate and automate third-party management is vital.

The right technology solution serves as a common platform to manage multiple third parties and provide better visibility into risk and compliance issues.

CONCLUSION

As the outsourced environment continues to grow and expand, protecting company assets and reputation becomes ever more rigorous and complex. Leveraging this checklist to develop or update third-party security best practices within a TPM program will help to protect your organization from cyberattacks, safeguarding corporate reputation while positioning your organization to thrive in an increasingly interconnected environment.



AVERTIUM

Avertium is the foremost provider of security and compliance consulting services to the midmarket and enterprise. The company's team of highly certified security experts serves more than 1,200 customers in the technology, healthcare, retail, hospitality, financial services and manufacturing sectors nationwide. Customers enjoy 24/7/365 monitoring from dual security operation centers in Arizona and Tennessee.

Founded in 2019 when award-winning cybersecurity companies Terra Verde Security, TruShield and Sword & Shield Enterprise Security were acquired by Sunstone Partners, a leading growth equity firm, Avertium is on a mission to make its customers' world a safer place.

20601 N 19th Street, Suite 150,
Phoenix, Arizona 85027

+ 1(877)-707-7997

hello@avertium.com
www.avertium.com

v03_2020