White Paper

VMware and the Need for Cyber Supply Chain Security Assurance

By Jon Oltsik, Senior Principal Analyst

September 2015

This ESG White Paper was commissioned by VMware and is distributed under license from ESG.

Contents

Executive Summary 3

Cyber Supply Chain Security Realities 3

Cyber Supply Chain Security Can Be Difficult 4

CISOs are Bolstering Cyber Supply Chain Security Oversight 5

Cyber Supply Chain Security Assurance 7

The VMware Trust & Assurance Framework 8

The Bigger Truth 10

Executive Summary

The common saying, "may you live in interesting times" is actually the English translation of a traditional Chinese curse. This reality is somewhat ironic as CISOs and cybersecurity professionals would likely agree that they indeed live in a very interesting but difficult time. Why? Cyber threats have become more ubiquitous, stealthy, and targeted while the IT attack surface continues to expand, driven by cloud computing, Internet of Things (IoT) initiatives, and mobile application use.

Enterprise organizations now realize that we live in a unique time of increasing IT risk and are responding accordingly. Corporate executives and boards are participating more in their organizations' cybersecurity strategies to mitigate business and technology risk. Many firms have increased cybersecurity budgets as well and are now purchasing and deploying a potpourri of new security analytics systems and layers of defense.

All of this activity is a step in the right direction—but it is just not enough. VMware has introduced a new initiative called "VMware Trust and Assurance," which helps answer customers' questions about VMware's security and development practices and provides greater transparency around how it develops, builds, secures, and supports its applications.

This white paper concludes:

- **Organizations are exposed to vulnerabilities in the cyber supply chain.** The cyber supply chain introduces the risk that a product or service could be compromised by vulnerabilities and/or malicious code introduced advertently or inadvertently during product development or maintenance, due in part to increasing globalization of the IT supply chain. Consequently, IT products and services built on a foundation of broad diverse cyber supply chains may increase the risk of a devastating cyber-attack to customers.
- **IT risks are not limited to corporate LANs, WANs, and data centers.** Rather, enterprises remain at risk for cyber-attacks that take advantage of vulnerabilities existing in IT equipment, business partner networks, non-employee devices, etc. As the saying goes, "the cybersecurity chain is only as strong as its weakest link." Regrettably, much of the cybersecurity chain resides outside the perimeter firewall and thus needs proper oversight, cybersecurity best practices, and ample layers of defense.
- **CISOs are pushing back on IT vendors.** Pragmatic cybersecurity professionals now realize that their strategic IT vendors can make or break the cybersecurity chain. In the worst case, insecure partners or IT systems can be used as a staging ground for a devastating data breach. To minimize risk, many enterprise organizations are addressing cyber supply chain security by auditing IT vendors' security processes and making purchasing decisions based upon a vendor's ability to meet increasingly rigorous cybersecurity requirements.
- **IT vendors must develop cyber supply chain security assurance capabilities; The VMware Trust and Assurance Framework serves as a model for the industry**. Enterprise cybersecurity requirements will continue to become more rigid in the future. As this situation evolves, CISOs will only do business with trusted IT vendors with demonstrable cyber supply chain security assurance programs that include all aspects of their product development, testing, distribution, deployment, customization, and support. VMware's Trust & Assurance initiative serves as a model of the transparency needed for cyber supply chain security for the industry. CISOs should demand a similar response from all strategic IT vendors.

Cyber Supply Chain Security Realities

Organizations large and small are changing their behavior with regards to cybersecurity in response to the increasingly dangerous threat landscape and highly-publicized data breaches. In fact, many organizations no longer consider cybersecurity an IT issue alone. Alternatively, cybersecurity risk is now a business priority that gets ample attention with business executives and corporate boards. According to ESG research:

- When asked to identify the biggest driver for technology spending over the next 12 months, 46% of organizations pointed to security and risk management initiatives. This was the most popular response, quite a bit higher than the second most popular answer, "cost reduction initiatives," which came in at 37%.
- Just over one-third of organizations (34%) say that Information security initiatives are the most important IT priority this year. Once again, this was the top response.
- 59% of organizations said that their IT security budgets for 2015 would increase while only 9% said they would decrease infosec budgets this year.[1]

Increasing focus on cybersecurity has resulted in lots of activity, as many organizations add layers of defense to their networks, implement new solutions for incident detection and response, and bolster security monitoring and analytics efforts. These internal efforts are a good start but a growing number of CISOs realize that cybersecurity risk extends beyond the LAN, WAN, and corporate data centers to a larger population of customers, suppliers, and business partners. This larger cybersecurity universe is sometimes referred to as the cyber supply chain, which ESG defines as:

"The entire set of key actors involved with/using cyber infrastructure: system end-users, policy makers, acquisition specialists, system integrators, network providers, and software hardware suppliers. These users/providers' organizational and process-level interactions to plan, build, manage, maintain, and defend cyber infrastructure."

Cyber supply chain security issues are not uncommon. For example:

- In 2008, the FBI seized $76 million of counterfeit Cisco equipment.
- As part of the Stuxnet incident in 2010, five companies acting as contractors for the Iranian nuclear program had their networks compromised in order to gain trusted access to government nuclear facilities.
- The successful 2013 data breach at Target Corporation was eventually traced to system compromises at Fazio Brothers, one of Target's HVAC contractors. Hackers used Fazio Brothers as a staging ground and used the company's network access as an attack vector.

Cyber Supply Chain Security Can Be Difficult

Some CISOs recognize the risks associated with their cyber supply chain security and this is especially true for organizations that depend upon armies of external business partners, contractors, or suppliers as part of their business operations.

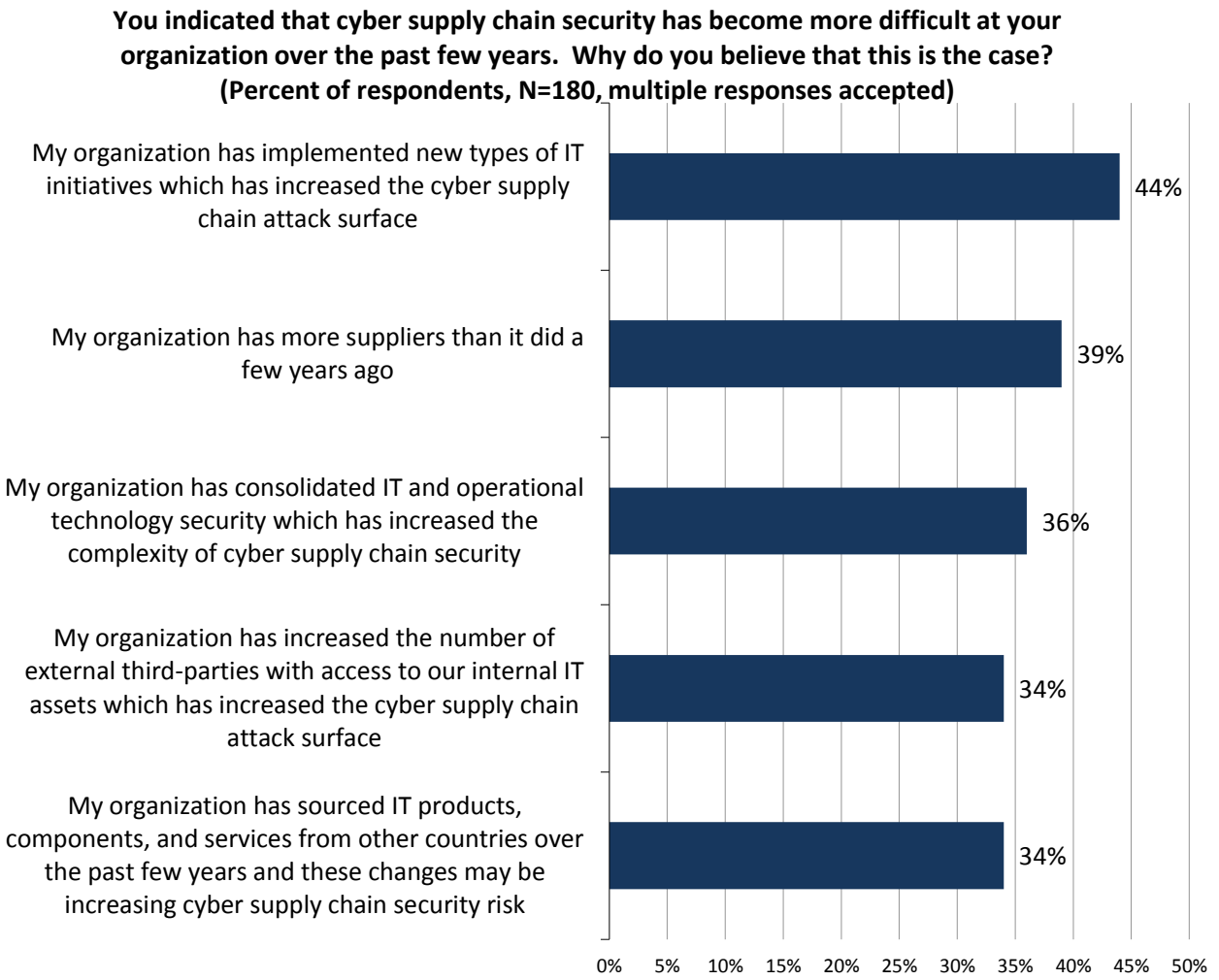
Unfortunately, cyber supply chain security best practices aren't easy as they require constant oversight of the state of cybersecurity related to IT equipment providers, software vendors, connected business partners, etc. In fact, cyber supply chain security seems to be growing increasingly problematic for some firms. In a recent ESG research survey of critical infrastructure sector organizations (i.e., chemical sector, emergency services, energy sector, financial services, health care, telecommunications, etc.), 40% of cybersecurity professionals admitted that cyber supply chain security has become more difficult over the past few years, and those who did supplied numerous reasons for that increased difficulty (see Figure 1):

- 44% of critical infrastructure sector organizations say that their organization has implemented new types of IT initiatives, increasing the cyber supply chain attack surface. These initiatives include BYOD, cloud computing, Internet of Things (IoT) projects, and the growing use of mobile applications and devices.
- 39% of critical infrastructure sector organizations say their organization has more suppliers than it did two years ago. This is to be expected, given the wave of IT innovation around software-defined data centers, cloud platforms, virtual networks, etc.
- 36% of critical infrastructure sector organizations say that their organization has consolidated IT and operational technology (OT), increasing the complexity of cyber supply chain security. In these cases, CISOs

[1] Source: ESG Research Report, *2015 IT Spending Intentions Survey,* February 2015.

are forced to secure business-critical but unfamiliar technologies like programmable logic controllers (PLCs) and supervisory control and data acquisition (SCADA) systems used for industrial operations.[2]

Figure 1. Reasons Why Cyber Supply Chain Security Has Become More Difficult



Source: Enterprise Strategy Group, 2015.

Aside from the assortment of issues described in Figure 1, CISOs often voice other concerns to ESG. For example, many security executives are anxious about the growing use of open source components (and vulnerabilities) as part of commercial software (i.e., Heartbleed, OpenSSL, Shellshock, etc.). CISOs also worry about things like rogue insiders working for IT suppliers and data privacy related to sensitive information moved to the cloud by IT vendors and business partners. Data privacy and cyber supply chain security issues can also be a source concern driven by global "follow-the-sun" development practices and cloud architectures, as well as emerging regulations like the EU Digital Single Market initiative.

CISOs are Bolstering Cyber Supply Chain Security Oversight

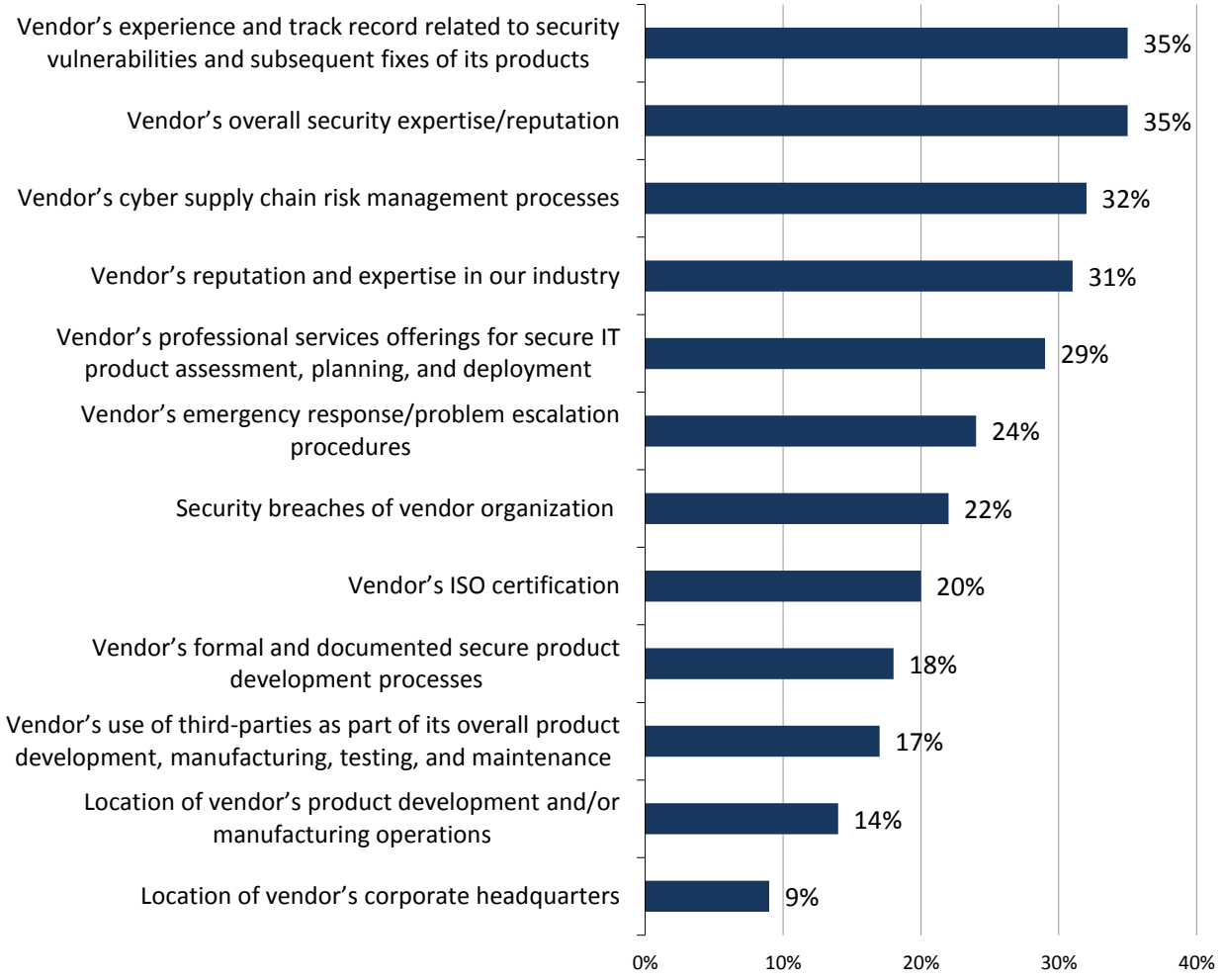
As cybersecurity morphs from a technology to a business issue, CEOs and corporate boards are gaining a better perspective of cyber supply chain security risks. This is driving a chain reaction—business executives are pushing CISOs to mitigate cyber supply chain risk, causing cybersecurity executives and purchasing managers to place more stringent cybersecurity requirements on their IT vendors.

[2] Source: ESG Research Report, *Cyber Supply Chain Security Revisited*, September 2015. All ESG research references and charts in this white paper have been taken from this research report unless otherwise noted.

ESG research illustrates this trend with an extensive array of security considerations for IT vendors as critical infrastructure sector organizations evaluate and purchase IT products and services. For example, 35% examine a vendor's experience and track record related to security vulnerabilities and software patches, 35% look at a vendor's overall security expertise and reputation, and 32% contemplate a vendor's reputation and industry expertise (see Figure 2).

Figure 2. Cybersecurity Evaluation Considerations for IT Purchasing of Products and Services

The following is a list of security considerations an organization may evaluate before purchasing IT products and services. Which of the following considerations are most important to your organization during the product evaluation and purchase process? (Percent of respondents, N=303, three responses accepted per respondent)



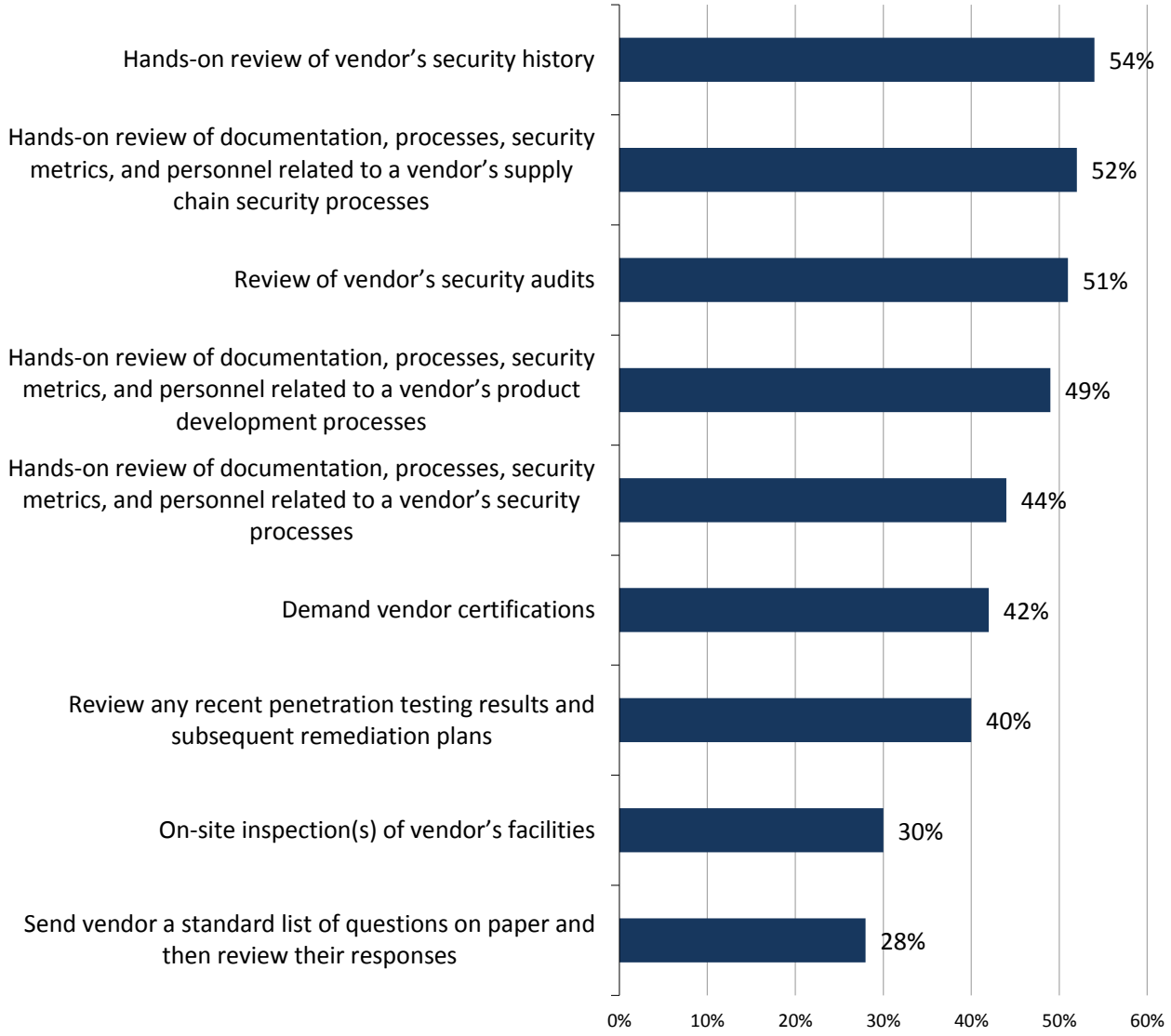
Source: Enterprise Strategy Group, 2015.

To further appraise IT vendor security, many organizations are also adopting a formal cybersecurity audit process as part of their IT procurement process. For example, 91% of critical infrastructure sector organizations audit the cybersecurity of their strategic software vendors (i.e., always conduct audits or do so on an as-needed basis), 90% audit the cybersecurity of their cloud service providers, and 88% audit the cybersecurity of their strategic IT infrastructure vendors.

These audits are becoming increasingly comprehensive. As ESG research illustrates, IT vendor cybersecurity audits include things like hands on reviews of a vendor's security history, reviews of a vendor's security documentation, processes, and metrics, and reviews of vendors' own internal IT and compliance audits (see Figure 3).

Figure 3. Mechanisms Used In IT Vendor Audits

You have indicated that your organization conducts audits of its IT vendors' security processes. Which of the following mechanisms does your organization use to conduct these IT vendor security audits? (Percent of respondents, N=294, multiple responses accepted)



Source: Enterprise Strategy Group, 2015.

Cyber Supply Chain Security Assurance

The ESG research presents a clear picture—high-security enterprise organizations are increasingly demanding greater cybersecurity best practices from their strategic IT vendors. Furthermore, vendors' cybersecurity policies, processes, and metrics are becoming a determining factor for IT procurement as advanced organizations are now selecting strategic IT vendors based upon a new standard, cyber supply chain security assurance, defined as:

Cyber supply chain security assurance *is the practice of managing cyber supply chain risks related to the people, processes, and technologies used to design, develop, produce, distribute, and implement IT hardware, software, and services.*

To parse this definition further, cyber supply chain security assurance includes:

- **Secure product development.** This includes a secure software development lifecycle, assessment, and testing of open source and third party code included in vendor products, and consideration of the cybersecurity practices of all contractors and suppliers that participate in software development or hardware bill of materials.
- **Adequate security skills.** To minimize risks associated with human error, product developers, testers, and other handlers must have suitable and up-to-date cybersecurity skills.
- **The right cybersecurity processes and procedures.** Vendors must back their day-to-day operations with cybersecurity best practices for risk management, threat prevention, and incident response. Additionally, IT vendors must employ cybersecurity best practices for internal IT themselves.
- **Field-level cybersecurity expertise.** Even when cybersecurity features are embedded in IT systems, overwhelmed customers may not know how to configure devices or customize systems for their individual security needs. Vendors with leading cyber supply chain security assurance skills have field-level employees or partners who can help customers consume and benefit from product security features and functionality upon deployment and continually over time.
- **Strong cybersecurity customer support.** While vendors should do all they can to develop, distribute, and deploy secure products, they also must have the right preparation for inevitable security vulnerabilities. Cyber supply chain security assurance demands that vendors' security teams monitor the latest attack trends and work with the greater security community to ensure timely awareness of new vulnerabilities that could impact their products. Once vulnerabilities are detected, vendors must also have highly efficient processes for developing, testing, and distributing software patches. Finally, vendors must have a highly trained staff to guide customers through security fixes as needed.

The VMware Trust & Assurance Framework

ESG believes that cyber supply chain security assurance is starting to have a market impact, creating a clear line of delineation between IT vendors with true cybersecurity commitments and those that remain behind. Sadly, many IT vendors have not embraced the right level of cyber supply chain security assurance, putting their customers at risk.

Since its formation in 1998, VMware Corporation has grown and evolved its role at enterprise organizations. Early on, VMware server virtualization technology was used primarily by IT departments for software testing and development. Over time, large organizations embraced VMware in production data centers for server consolidation. Most recently, VMware has become a strategic IT vendor at many enterprise organizations as VMware technology is often deployed on endpoints, in data centers, and across public and private cloud infrastructure.

As it advanced from tactical to strategic IT vendor, VMware faced a pattern of increasing cybersecurity scrutiny from demanding public and private sector customers. To address this, VMware management introduced an internal focus on continuous cybersecurity improvement several years ago. This effort culminated recently with an initiative called VMware Trust & Assurance, which is composed of four guiding principles:

- **Reliability.** Within the VMware Trust & Assurance framework, the commitment to reliability includes:
    - Product performance and scalability in order to ensure that VMware products can meet enterprise demands.
    - A pervasive culture of evangelism and education to keep VMware employees and customers educated and engaged on rapidly-changing cybersecurity risks.

  - Research dedicated to enhancing VMware product performance and reliability while working with customers on associated project planning, testing, deployment, and optimization.
  - Quality metrics and continuous improvement associated with VMware products, people, and partners.
- **Integrity.** This principle aligns with VMware's software development and comprises:
  - The VMware software development lifecycle. VMware had built a development process that includes formal repeatable processes for software design, testing, documentation, release, and ongoing support.
  - Compliance and risk. Along with its partners, VMware developed the compliance reference architecture framework (RAF) that aligns its technology with regulatory compliance requirements across industries.
  - Software supply chain management. VMware is addressing its own cyber supply chain practices in a number of areas including IP protection, source code sharing, risk management assessment, and proactive software security programs with strategic partners and suppliers.
  - Privacy. To protect customer privacy, VMware defines its privacy policy to customers, specifying what data it collects and how it is used. VMware follows a "privacy by design" framework to provide transparency on privacy as it relates to products, services, and support.
- **Security.** VMware has introduced strong cybersecurity throughout its organization. Examples of this include:
  - Product security. VMware has created a product security team responsible for oversight of all product security. This group supervises security development processes and metrics with each product team and is responsible for demonstrating continuous improvement.
  - Security development lifecycle. This extends beyond the secure software development lifecycle and includes security training, planning, serviceability, as well as response planning, product security requirements assessment, and overall security monitoring.
  - The security response center. VMware employs a team of security researchers, software developers, and support staff to find vulnerabilities, develop fixes, and work with customers and partners for timely distribution and deployment of security fixes.
  - IT security. Like all large enterprises, VMware's corporate infrastructure is under continual attacks from malicious individuals and entities. To address this risk, VMware maintains cybersecurity best practices on internal networks and systems.
- **Commitment.** To make cyber supply chain security assurance pervasive in everything it does, VMware has made cybersecurity part of its corporate culture. Of course, this requires a true cybersecurity commitment including:
  - Continuing product development. VMware has established a continuing product development organization, which acts as a single point-of-contact for addressing, escalating, and resolving product and customer cybersecurity issues.
  - Ecosystem services. VMware understands that its cyber security supply chain includes a network of hundreds of other IT vendor and services partners. VMware provides technical support, testing, cooperative support services, and rules-of-engagement to ensure strong cybersecurity in the field.
  - Customer advocacy. VMware recognizes that cybersecurity professionals are a community of like-minded individuals with a few common goals—mitigating IT risk and protecting critical IT assets and data. To succeed, VMware depends upon a partnership of equals with VMware

participating in the cybersecurity community rather than dictating its own IT vendor agenda. VMware seeks to facilitate this relationship with security research, workshops, benchmarks, security education, and social media campaigns.

With its Trust & Assurance initiative, VMware is taking a 360 degree perspective on cybersecurity that encompasses its products, partners, customers, employees, and the cybersecurity community at large. In this way, VMware has not only responded to its enterprise customers' need for greater transparency related to cyber supply chain security, but is also setting an example that should be emulated by other IT vendors.

The Bigger Truth

CISOs face a daunting area of challenges. Cyber threats grow more voluminous, sophisticated, and targeted while IT infrastructure gets more complex as network perimeters disappear. Yes, these changes demand an increasing commitment to cybersecurity oversight, risk management, and tight security controls but these efforts simply can't be limited to corporate LANs, WANs, and data centers. Rather, CISOs must understand the risks associated with their cyber supply chains, and establish best practices for cyber supply chain security.

ESG research indicates that this transition is already in progress, causing many organizations to audit the security of their IT product and services vendors. Leading edge enterprises are also making purchasing decisions based upon their vendors' cyber supply chain security assurance programs. Moving forward, more organizations will likely follow suit.

Unlike many other enterprise IT vendors, VMware is well prepared for this increasing level of cybersecurity oversight. In fact, the VMware Trust & Assurance initiative is designed to meet and exceed the growing need for greater transparency related to enterprise cybersecurity. As such, VMware is setting an example for the IT industry at large. CISOs would be well served to demand similar cyber supply chain security assurance from ALL of their strategic IT vendors.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com