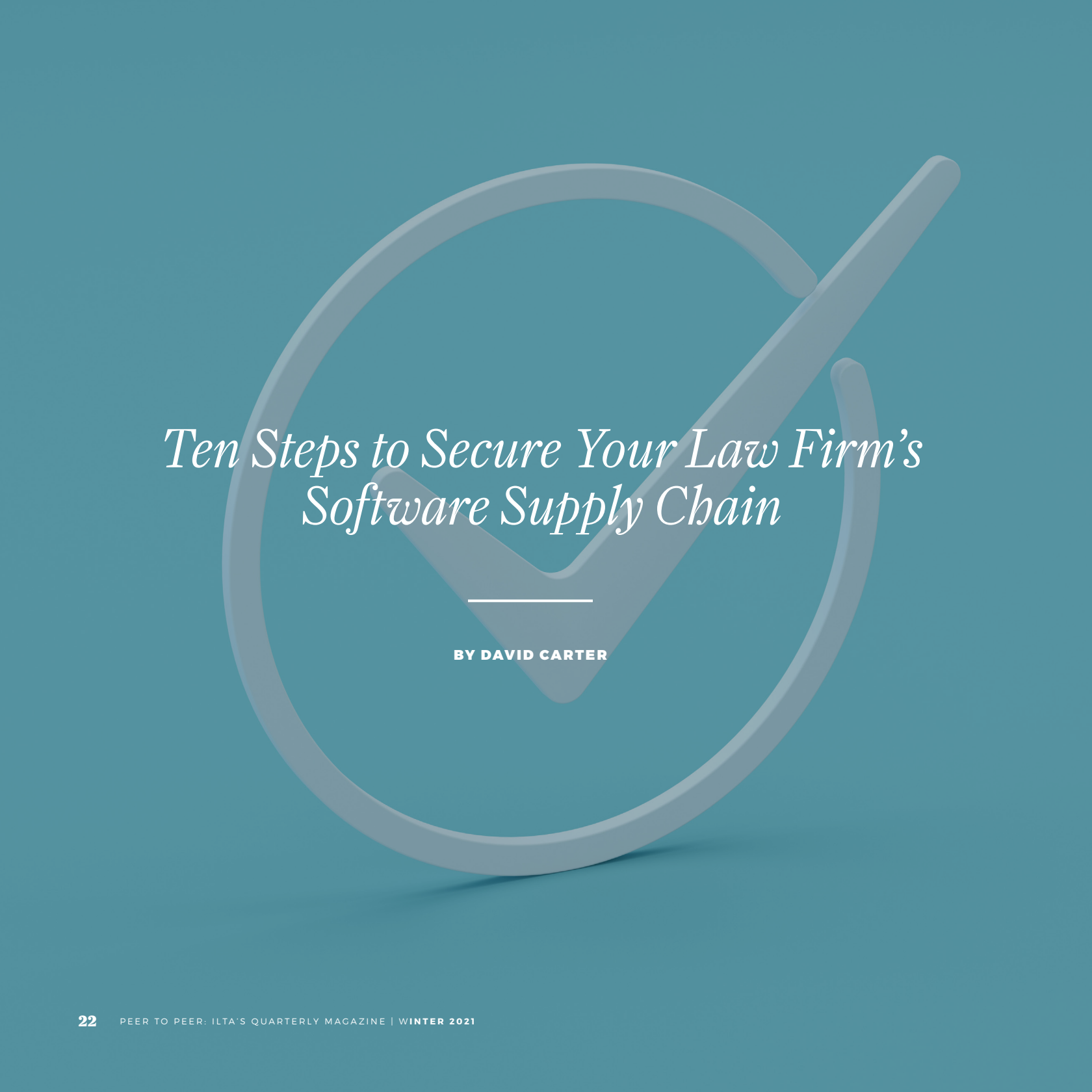
ISSUE #4 | VOL. 37

Peer to Peer

ILTA'S QUARTERLY MAGAZINE

Maturity and Security:

LEGAL AND LAW DEPARTMENTS IN THE 21ST CENTURY



Ten Steps to Secure Your Law Firm's Software Supply Chain

BY DAVID CARTER

Law firms face unique challenges when it comes to security. Not only must they safeguard their own internal data, but they must also ensure that confidential client documents are stored securely. The risks and responsibilities regarding data management are substantial, and the penalties imposed for errors are stiff. While software solutions are essential to a firm's daily operations, technology and tech vendors can pose significant security risks. Ensuring the security of a firm's software supply chain is, therefore, a critical objective.

In the 2020 SolarWinds hack, attackers compromised the technology company by inserting malicious code into their security monitoring platform. A "back door" was inserted into SolarWinds' popular monitoring suite allowing attackers to infiltrate thousands of networks in the public and private sectors, negatively impacting their customers.

The SolarWinds breach serves as a cautionary tale, demonstrating that all organizations— including law firms— must be vigilant when securing their on-premise technology and software-as-a-service (SaaS) supply chain. Security for the entire legal software supply chain is more vital than ever. Firms now frequently perform IT and business functions remotely, and more firms use cloud-based solutions due to the ongoing pandemic. Because many firms have plans to move to the cloud and migrate from on-premise products to SaaS solutions in the future, they will soon have broader security considerations.

A law firm's software supply chain includes all locally installed desktop and server computer software and cloud/SaaS technology delivered over the internet. It also has an often-overlooked layer: the vendors used by the technology suppliers, who must be evaluated for risk and compliance assurance.

The **Cyber Supply Chain Risk Management Practices for Systems and Organizations**, a publication from the US government entity **NIST** (National Institute of Standards and Technology), provides a strong foundation for law firms evaluating their supply chain security practices. As an additional step for law firm CIOs and IT Directors tasked with securing their legal software supply chains, the following checklist serves as a guide of best practices recommendations.

The IT Checklist for Securing a Law Firm's Software Supply Chain

1. Identify and Inventory

First, identify the scope of the firm's software supply chain. Take an inventory of all the software the firm is using to understand the total software footprint. Firms must have a comprehensive understanding of all devices and software they rely on for their business operations.

Law firm IT staff will likely be surprised by the average number of vulnerabilities detected per device, which can total well into the thousands even after addressing the most critical vulnerabilities. Every laptop, desktop, tablet, and smartphone contains applications that must be inventoried to understand the scope of the problem.

Firms may be unpleasantly surprised to find that users have downloaded, trialed, and purchased products without IT's knowledge or authorization. Making a comprehensive inventory requires IT to turn over many rocks to discover what lies beneath.

Once drafted, the inventory list can be overwhelming. Because security concerns will differ, consider dividing the list into categories, perhaps separating by practice area, office location, and on-premise desktop software versus SaaS systems. Also, note which package and version numbers are used for each software product and update them when applying patches and upgrades. Create a monthly or quarterly schedule to update the inventory since it will continuously evolve.

Commercial software packages are available to perform ongoing hardware and software inventory scanning. Firms may find that implementing an automated inventory scanning solution is cost-justified when labor savings and risk reduction are considered.

2. Expand the Net

Once you have your initial inventory of software used across the firm, think bigger. The costliest cyber breaches occurred when businesses did not think "out of the box" to discover overlooked security risks and were subsequently blindsided.

For example, Home Depot paid $17.5 million to settle a data breach lawsuit that originated from hackers using a vendor's username and password to infiltrate the company's network.

Target was hit by hackers who infiltrated its systems by using the network credentials of a third-party HVAC and refrigeration subcontractor. As a result, Target paid $18.5 million to settle claims from 47 states and the District of Columbia.

Even technology hardware as commonplace (and seemingly harmless) as keypad door entry systems in offices has a web-based administrative console maintained by a SaaS interface. Some of these systems lack support for essential security capabilities such as multifactor authentication. Commonplace office items, including access control keypads, printers, and copiers, are easy to miss when compiling an inventory, but they can present real security vulnerabilities for the firm. Learn from other companies' misfortunes by making your security net wider – when in doubt, include and plan to protect everything.

3. Examine Your Processes and Go Deeper

Look at the various processes throughout your firm, within the law practice, accounting, human resources, IT, and more. Each process has its own software supply chain, including a mixture of technology locally installed on desktop computers and cloud-based/SaaS tech delivered over the internet. However, this is just the first level— go deeper than just the firm's direct vendors and include their suppliers. For example, the firm's software providers may license or embed other companies' code in their technology. Additionally, if the firm's software suppliers have access to your network and data with inadequate security protection, their breaches could affect the firm's data. The firm's security should be rigorous, covering both their direct software suppliers and the third-party companies that service those vendors, too.

4. Formulate a Vendor Risk Management Process

Implementing a strong vendor risk management process is essential to protect the firm. Questionnaire templates such as SIG (Standardized Information Gathering) and the abbreviated SIG Lite can provide a framework and sample questions to assist the firm in developing its questionnaires for existing and new vendors.

Questionnaires can verify the vendor's defense networks, cloud security practices, software development lifecycle controls (for tech providers), their use of monitoring and scanning tools to detect vulnerabilities, and their history of breaches and security incidents. Ask about the credentials they require for data access, including how they are protecting passwords and ensuring their system is only accessed by authorized parties. Security-related evaluation questions should be embedded in the firm's RFPs (requests for proposal) and purchasing process to vet all suppliers vying to do business with the firm.

5. Perform Risk Triage and Evaluation

Once vendors have responded to risk management questionnaires, IT can then evaluate them to flag the

security risks each one poses. Some vendors may pose a higher risk, particularly if they have access to sensitive or confidential information regarding the firm or its clients. The firm must determine whether remediation measures can mitigate these risks, whether the risk level is tolerable based on what product/service is being provided, or whether the vendor must be declined.

Software vendors must be held to a higher standard than many other suppliers since they are often deeply entrenched in the firm's infrastructure and have remote access to the firm's network. When buying software, be sure to have a risk/compliance professional assist with compiling and reviewing risk management questionnaires.

6. Weigh Risks Against Business Necessity

Remember that standard questionnaires are aspirational; no vendor response is ever 100% perfect. The firm's IT security and risk management professionals must review vendors' security credentials and then apply their judgment to the assessment.

The firm may accept a greater level of risk for a specific vendor depending on how vital the vendor's product/service is, weighed against the potential risks to the firm. Vendors handling confidential or sensitive material for the firm, such as personally identifiable information (PII), credit card information, or privileged material, are held to a higher security standard because the risks are more significant.

7. Require Security Tools for Software Vendors

Monitoring and Scanning – A firm's risk management questionnaire can include questions about the security technology tools the software vendor uses to monitor and detect vulnerabilities and anomalous activity. Ideally, software companies have deployed a suite of tools to scan their computers and services and detect vulnerabilities in code. This standard applies to both on-premise and cloud tech suppliers. Scanning and monitoring tools can also detect malicious code in PDF files and email messages, among the most common vehicles for bad actors to embed viruses or other harmful code.

Security Agents – There are many links in the software supply chain, and weaker points give bad actors paths to intrude. Software providers can have a security agent sitting on each machine to detect anomalous/strange activity and shut down the activity immediately. Are the firm's devices being used to reach out to servers in countries with known cybercriminal activity, such as China, Nigeria, and Russia? Are machines making requests to strange websites? Security agent technologies slam the door on malicious servers and agents. Having security agents and the scanning/monitoring tools in place creates in-depth defense to block nefarious activity.

Firewalls and Perimeter Defense – Network firewalls, web application firewalls, and similar devices form a frontline of defense for your vendors' networks. Ensure that your vendors are as vigilant in protecting their network as you are about protecting your own. This is especially important if the vendor can remotely access your networks since a compromise of your vendor's network could lead to unauthorized access of yours.

8. Create a Remediation Plan

If a firm truly needs a vendor's product or services, but the supplier's security questionnaire is not satisfactory, law firm security managers, CIOs, and IT directors can start a dialogue with the vendor to create a remediation plan. The firm can assist vendors in setting objectives and timelines. Then, the vendor can be held accountable for making necessary security improvements to meet the firm's specifications.

9. Monitor and Adapt to Problems as They Arise

New security issues surface daily, so law firm IT will continually prioritize, troubleshoot, and remediate problems as they are discovered. The supply chain inventory will grow and change. Vendor responses to questionnaires will change over time, so stay in touch with suppliers regularly. Software supply chain security is an eternal "rinse and repeat" process, so establish a routine around it that is flexible enough to incorporate new software products and address security threats that enter the environment.

10. Regularly Brief Business Leaders

Law firm executive leadership looks to IT for guidance and accountability on security issues. Be sure to keep top executives informed about security, including the vetting of major new vendors and notification of data leaks or breaches. Establishing regular communication,

including periodic reports and check-in meetings, keeps firm executives informed and reinforces IT's reputation as accountable, prepared, and responsible when it comes to securing the software supply chain. Develop a process for notifying executives if a breach occurs via a software vendor and a cyber incident response process and revise those processes over time as needed. Instill confidence in the firm's leadership that IT is protecting the firm and its assets. These steps will assist IT in requesting any additional budget required to keep the firm and its clients safe from security threats.

Law firms have the herculean task of ensuring the security of their software supply chain. By understanding what software the firm relies upon, firms can better define the scope of their vendor risk management programs. Firms should engage their software vendors as allies in this process, ensuring that they have appropriate security controls in place and provide accountability to their law firm customers. By following the above checklist, law firm IT professionals can keep the firm secure and reinforce their value to the firm's leadership. **ILTA**

David Carter *is the Chief Information Officer (CIO) at Aderant, an ILTA Platinum sponsor and global industry-leading business management software provider for law firms. David has an in-depth background in on-premise and cloud-based/SaaS technology management and support, having worked at mainstream tech providers and consulting firms, including Unisys, S1 Corporation, and Accenture, before joining Aderant. He holds a Bachelor of Science in Business Administration from the University of Alabama and an MBA from the University of Chicago's Booth School of Business.*

ILTA TV

SPOTLIGHT ILTACON EDITION

Check out our ILTA TV News segment with David Forrestall, SecurIT360!