ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

4 Best Practices for Third-Party Threats

Commercial and Contracts

Law Department Management

Technology, Privacy, and eCommerce

Corporate, Securities, and Governance

CHEAT SHEET

***Constant challenge*.** Third-party threats — whether from the supply chain or a service provider — are one of the most significant risks facing companies today and need to be continuously monitored.

***Due diligence*.** Companies need to examine — and reexamine — their vendors over the course of the relationship in order to protect their data, clients, and supply chain.

***Active management*.** By incorporating privacy and security requirements into third-party contracts, in-house counsel can hold third parties accountable, reducing the risk of unilateral changes by these third parties without your affirmative consent.

***C3POO*.** Someone in the C-suite needs to take ownership of third-party threats, such as a Chief Third-Party Oversight Officer.

By all accounts, 2020 was a challenging year, and it was no less interesting from a cyber and privacy perspective. It started off with fears of a major cyber intrusion of our critical infrastructures. But that soon faded into the background as the COVID-19 pandemic took center-stage. The nationwide shift to remote work led to an exponential increase in phishing and ransomware attacks, as well as an appreciable increase in nation-state intrusions targeting academic, governmental, and private sector entities seeking intelligence on vaccine development efforts. And of course, who can forget Russia’s cyber finale to the year, better known as the SolarWinds hack.

2020 was also the year that third-party providers took a more prominent place in our collective consciousness. We've heard warnings about third-party supply chain vulnerabilities as far back as 2013 when a hack compromised Target's third-party refrigeration contractor and allowed attackers to load malware to nearly all of Target's US point-of-sale machines, stealing millions of credit and debit card numbers.

In another example of a third-party vulnerability, Chinese residents and nationals were recently indicted by the Department of Justice (DOJ) for supply chain hacking on behalf of the Chinese government. According to DOJ, "the hackers compromised software providers and then modified the providers' code to facilitate further intrusions against the software providers' customers." More recently, the SolarWinds breach highlighted the dangers of third-party supply chain vulnerabilities, as intruders penetrated SolarWinds systems, injecting "malicious code into the patches of SolarWinds' Orion product."

The *Financial Times* reported that "as some 18,000 SolarWinds clients updated their software, they unwittingly introduced a hidden backdoor," that went undiscovered for six to nine months. And while it's true that SolarWinds arguably represented a failure of our intelligence agencies to identify the attack, the proximate cause of the attack was a vulnerability caused by the use of a third-party in the supply chain.

> Third-party providers today have become integral to many of our business processes.

But 2020 also bore witness to a great deal of third-party vulnerabilities from the privacy perspective. For example, General Electric (GE) suffered a breach in February 2020 through its third-party contractor Canon Business Process Services (CBPS), which specializes in outsourced human resources tasks like accounts payable, reportedly exposing direct deposit and tax forms, scans of birth certificates and passports, court orders and photos of driver's licenses. And in November 2020, Spain-based third-party provider Prestige Software, whose software connects online reservations sites like Expedia and Booking.com with hotels, leaked years of sensitive Personally Identifiable Information (PII) on hotel guests and travel agents.

2020 then culminated with the FTC's proposed settlement with Texas-based mortgage analytics company Ascension Data & Analytics, penalizing Ascension for having failed to properly oversee its third-party vendors by failing to ensure that they implemented and maintained "appropriate safeguards for customer information," and failing to mandate those requirements by contract.

Bottom line is that third-party providers today have become integral to many of our business processes. But with that dependency, these third parties have increasingly introduced risk from both a cybersecurity and privacy perspective. Indeed, in recognition of this fact,

NIST added a set of “Supply Chain Risk Management” controls to its Cybersecurity Framework in 2018. And NIST’s Privacy Framework, issued in January 2020, likewise addresses third-party risks as part of its overall enterprise risk management approach.

Consider ransomware attacks. Traditionally, ransomware attacks were limited to infecting a system, encrypting the data, and holding the decryption key for ransom. It was a cybersecurity incident. But in 2020, ransomware transformed to a hybrid exploit, with the perpetrator double dipping, holding both decryption keys and PII and proprietary information for ransom. In other words, it’s now both a cybersecurity incident and a privacy breach. And while we’re still trying to ascertain exactly what was taken in the SolarWinds hack, there’s a good likelihood that PII was stolen.

Patchwork of requirements

Exacerbating the cybersecurity and privacy dangers that third-parties pose today, there is a lack of clear and consistent guidance governing their oversight, with a patchwork of requirements showing up in a range of laws, regulations, and frameworks. For example, there are industry-specific requirements for third-party providers, such as the GLB requirements referenced in the FTC’s action against Ascension. And then of course there’s the Security and Privacy Rules under the Health Insurance Portability and Accountability Act (HIPAA) which, through the HITECH Act, are incumbent on third-party providers (Business Associates) used by HIPAA-covered entities. There are also state-specific laws, such as New York’s Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which requires covered organizations to select “service providers capable of maintaining appropriate safeguards, and requiring those safeguards by contract.”

Likewise, the recently passed California Privacy Rights Act (CPRA), designed to expand on the California Consumer Privacy Act (CCPA), mandates increased due diligence of third-party processing operations in order to improve the data supply chain through enhanced oversight. Sadly, purposefully absent from these new requirements is any recommendation for “specific contractual language” that might otherwise ensure responsible behavior by third parties.

And the NIST Privacy Framework requires that contracts with third-parties in the “data processing ecosystem” ensure appropriate measures to meet the needs of an organization’s privacy program, and that these third-parties be “routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their . . . obligations.”

Realistically speaking, however, these requirements are often very high-level, if not aspirational, without the detail needed to effect real change, not to mention consistency. The more effective way to address vulnerabilities presented by third parties from both a privacy and cybersecurity perspective would be to promulgate a set of common, consistent, and robust standards. In reviewing the requirements regarding oversight and management of third parties from various laws, regulations, and frameworks, four best practices become clear:

1. Due diligence throughout the relationship

The only way to confidently rely on a third party is through regular revalidation (annually, or at least bi-annually), using the same, robust due diligence process used when initially selecting that provider (as opposed to the one-and-done approach). Ronald Reagan called this “trust but verify,” but in today’s increasingly connected world, this is just common sense. After all, a provider’s sources change (e.g., parts originally secured from South America transition to being sourced from China because it’s

cheaper), cash flows change (leading to cuts in security processes that were potentially key in awarding the original contract), partners change, new website partner links are embedded on a site, potentially capturing visitor data and placing cookies without knowledge or consent, etc. And no organization wants to be the next Facebook dealing with another Cambridge Analytica.

Likewise, third-party data processors may change hosting services or data storage locations (governed by new laws and opening up new risks), their data sharing relationships may evolve, etc. The only way to ensure that the supply chain remains secure, and that private data remains private, is to regularly reassess third-party sources and risks.

Even once every year or two can provide significant improvement over the current box-checking mentality. After all, due diligence and audits of SolarWinds' security practices would likely have identified the vulnerabilities earlier, had someone looked. In particular, SolarWinds was owned and operated by a private equity firm focused on cost cutting, to include reducing or eliminating vital security precautions, lost its primary security executive because its approach to internal security was described as "catastrophic," and was alleged to have had such lax security that anyone could "access SolarWinds' update server by using the password 'solarwinds123.'" But since none of SolarWinds' clients had a mandate to perform due diligence after the initial agreement, no one discovered this vulnerability until it was too late.

2. Revalidation of all trusted security accesses

If the third-party provider has specialized access to your organization's systems, it's vital to revalidate that access annually, whether the service provided is software or hardware support/maintenance, an API plug-in (for ordering, shipping, credit card processing, etc.), data processing or storage services, etc. In this context, "specialized access" means access that circumvents your organization's security (firewalls, IDS, logins), or is pre-authorized to pass through your security without verification, such as through a specialized provider portal, direct access through a firewall exception, or through a special API interface. Relying on assurances of "Best in Class" or "Industry Leading" security practices is just so 2019.

As the civil liberties and privacy officer for the National Counterterrorism Center, we had an axiom when it came to privacy and security: If you're not seeing any incidents, you're either not checking, or you're checking for the wrong things.

> If you're not seeing any incidents, you're either not checking, or you're checking for the wrong things.

As such, you'll want to sample your logs relating to those accesses to ensure that the third party is only touching the data they should, and not accessing or removing the data they shouldn't. Part of this annual review process should also incorporate the question of whether the privileged access remains appropriate; it's not unheard of for a third-party relationship to end, but the privileged access provided to that third-party to remain in the system, creating a potentially unmonitored vulnerability.

Likewise, you should annually perform a deep dive into the provider's own processes for monitoring their privileged accesses to your systems. This deep dive should scrutinize records evidencing the third party's audits/spot checks of their access to your systems, documents relating to internal security or compliance reviews of incidents resulting from the access, and records demonstrating the third parties' validation of its security protocols and processes relating to that access (preferably by an outside security auditor). If the third party is hesitant to disclose compliance information, or lacks documentary evidence of compliance oversight and monitoring, you may want to rethink that third party's specialized access now, rather than after the eventual breach.

3. Active contract management

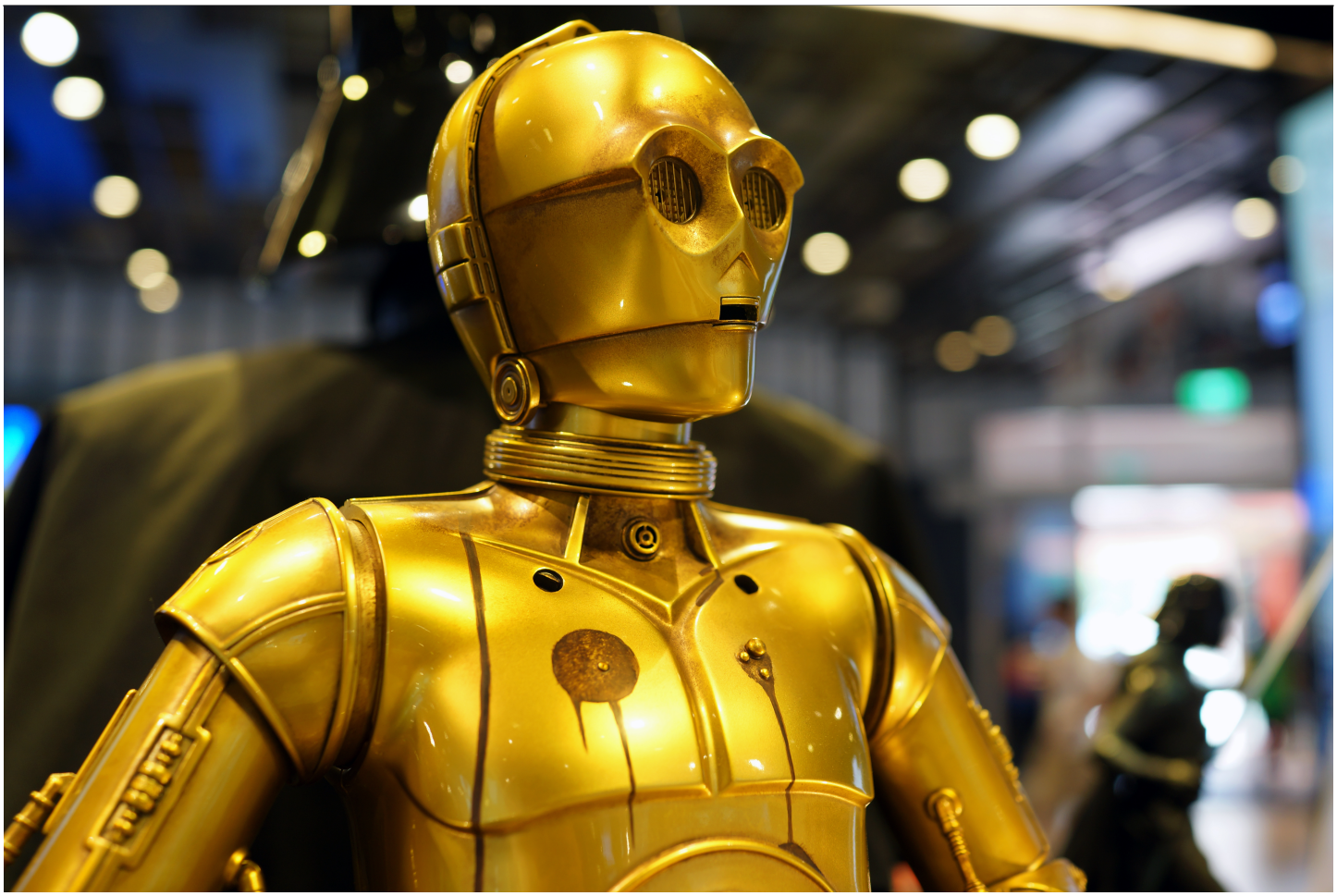
Security and privacy requirements/commitments should be explicitly incorporated into the provider contract in order to ensure that the third party adheres to the standards that led to their initial selection, as well as to any mitigation measures subsequently put in place to address issues uncovered during due diligence reviews. Unfortunately, it's often the case that the legal department is omitted during the revalidation phase, especially when an auto renewal clause kicks in. But as the old saying goes, this is penny wise and pound foolish. While it may take more time and incur additional legal cost (whether in-house or outside counsel), integrating these items into the contract will prove invaluable in the longer term; indeed, the FTC held Ascension liable under the Gramm-Leach-Bliley Act precisely because they failed to integrate these types of requirements into their contract with third-party providers.

Likewise, statutes like New York's SHIELD Act also explicitly require such requirements to be integrated into the contract. If the provider later wishes to make changes that affect the representations you relied upon, they will then need to inform you under the terms of the contract, and potentially amend the contract in order to make the change — as opposed to making the change unilaterally — providing a check and balance and keeping you actively apprised of material changes by the third-party.

4. C-suite accountability

Finally, someone in the organization should be ultimately responsible for overseeing all third-party relationships; supply chain providers and data processors, hosts, and storage providers. This person would conduct regular audits and compliance oversight, as well as ensure that all criteria identified during security access audits make it into the final contract. Ideally, this person would report to senior leadership, ensuring visibility and accountability from the top down. Perhaps it's time to add a new C to the C-suite, such as a Chief Third-Party Oversight Officer or C3POO (not to be confused with the Star Wars droid).

Interestingly, the GAO came to a similar conclusion in its December 2020 report to Congress on supply chain risks, noting that one of the "foundational practices" for properly managing supply chain risk is to establish "executive oversight of ICT activities, including designating responsibility for leading agency-wide SCRM [Supply Chain Risk Management] activities."



The C3POO — not to be confused with the Star Wars droid — would govern all third-party contracts.

At the end of the day, the practices discussed above are the ideal, and practically speaking, it may be challenging for every company to implement every requirement, with every third-party, every time. After all, if it were simple and cheap to do, we'd have seen these changes made a long time ago. In that case — and as discussed during the Supply Chain Risk Management Panel at the ACC's recent Cyber Summit — priority should be assigned based upon the criticality of the third party to the business. Which third-parties have access to large quantities of PII, or especially sensitive PII? Which parties are critical to keeping the lights on?

Realistically speaking, business executives will have to figure out which third-party providers to prioritize and scrutinize and in what order, a job well suited for our new C3POO. Most likely this will be based upon the service provided by the third party, the risk that corruption or exploitation of that third-party poses to the organization, and the potential damage that could ensue should that risk come to fruition.

What's becoming quite clear today, however, is that merely conducting due diligence once upon entering a new third-party agreement and then letting it ride for years just doesn't work anymore.

At the risk of sowing the very confusion I sought to avoid earlier, I find it necessary to quote the Star Wars droid himself, as C3PO wisely told R2D2, "You know better than to trust a strange computer." And indeed, we all do.

Joel Schwarz

Director, Privacy & Data Protection Lead

MBL Technologies

Joel Schwarz is a director, and privacy and data protection lead, for MBL Technologies, and an adjunct professor at Albany Law School, teaching courses on cybercrime, cybersecurity and privacy. He previously served as the Civil Liberties and Privacy Officer (CLPO) for the National Counterterrorism Center and was a cybercrime prosecutor for the US Department of Justice and NY State Attorney General’s Office. He was also counsel on e-commerce and privacy for MetLife.