October 2024

Third-Party Governance: Digital Identity

Jim Routh
Fellow, Institute for Critical Infrastructure Technology

www.icitech.org

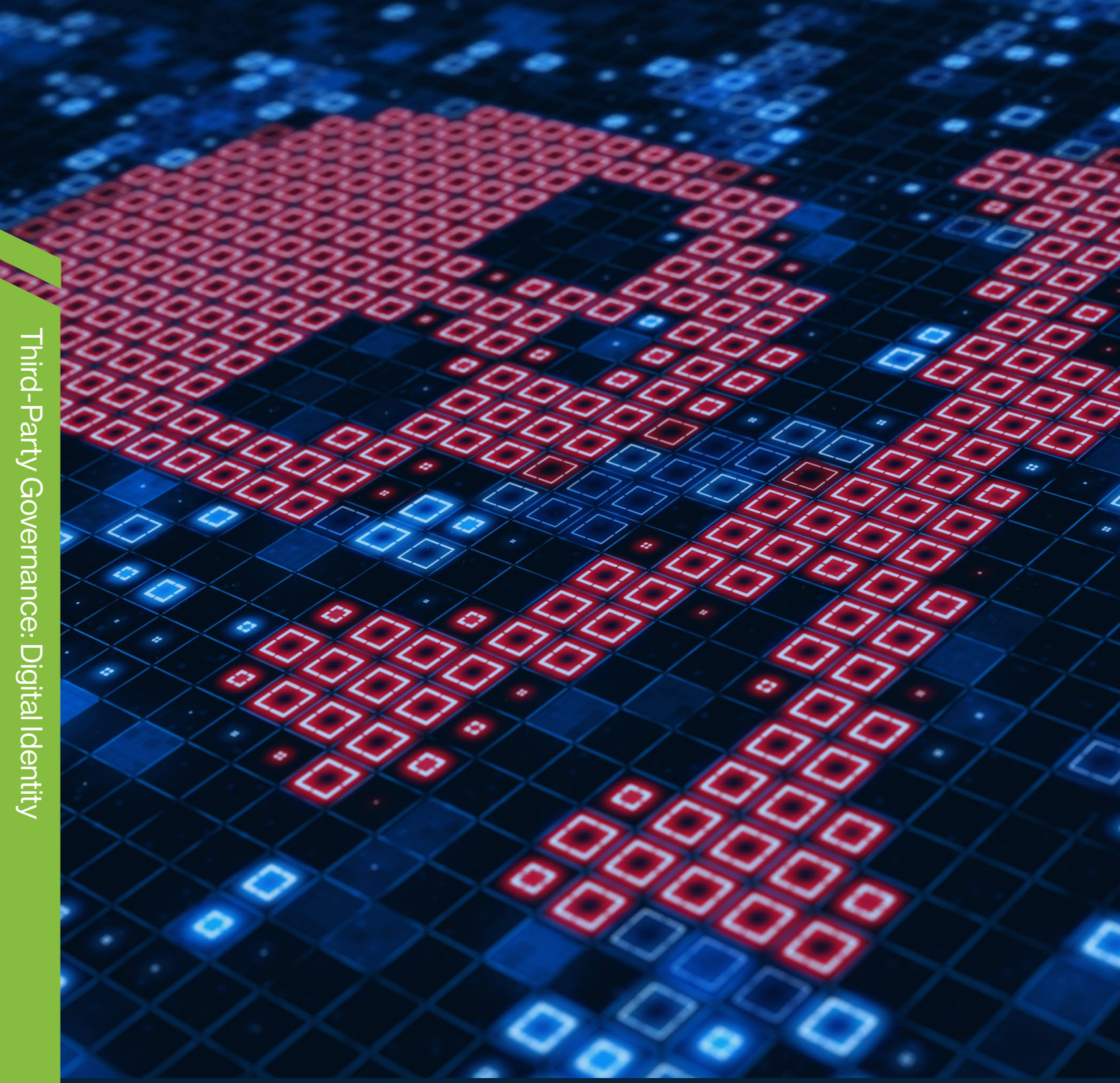
Table of **Contents**

About ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a nonprofit, nonpartisan, 501(c)3 think tank with the mission of modernizing, securing, and making resilient critical infrastructure that provides for people's foundational needs. ICIT takes no institutional positions on policy matters. Rather than advocate, ICIT is dedicated to being a resource for the organizations and communities that share our mission. The views and opinions expressed in this essay are solely those of the author(s) and do not necessarily reflect the official policy or position of ICIT. Any assumptions made within the analysis are not reflective of the position of any entity other than the author(s).

To learn more, please visit www.icitech.org

CyberRisk ALLIANCE | Thank you to our Strategic Partner **CyberRisk Alliance** | www.cyberriskalliance.com



Third-Party Governance

Digital Identity

There has been a noted increase in public data breaches originating from third-party suppliers in recent years. Many enterprises have been impacted by a single vendor compromise. In software supply chain compromises, the number of impacted enterprises can reach hundreds from a single third-party incident. For example, the Snowflake breach involved a systematic compromise of Snowflake customer instances using stolen customer credentials that impacted 165 enterprises.[1] The threat actor (UNC5537) created malware specifically designed to capture log in credentials.[2]

[1] https://www.threatdown.com/blog/snowflake-breach-looks-like-165-individual-incidents/ AT&T, Santander Bank, Advanced Auto Parts, Lending Tree, Live Nation, Neiman Marcus Group

[2] https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion Google-Mandiant analysis of threat actor for Snowflake incident

Learning from Incidents

CISOs often note the importance of learning from incidents, regardless of where they occur, or which enterprise is affected. This principle is often referred to as "never let a cybersecurity incident go to waste." Cybersecurity incidents provide valuable insights into which controls were effective and which ones failed. Mature cybersecurity programs investigate incidents inside their enterprise to apply the lessons learned and improve their own controls. However, accomplished cybersecurity leaders embrace the opportunity to learn from any incident in any enterprise. Any enterprise can almost always adjust controls base on wisdom gleaned from other's mistakes. The best-case scenario is applying the lessons learned from a cyber incident from another enterprise to your enterprise. Your enterprise benefits by reducing the probability of an incident without having to deal with the business impact of a cyber-attack

CrowdStrike's recent cybersecurity incident involved its endpoint protection software (Falcon Server) and caused significant business impact across enterprises and customers. CrowdStrike's CEO, George Kurtz, shared the post-incident review (PIR) information with customers and the public alike.[3] As a CISO for a cybersecurity product company, it is important to apply the lessons learned from the CrowdStrike incident to your own enterprise to avoid massive business disruption in the future. Specifically, software update testing should examine multiple use cases, including various user types, updates, "stress, fuzzing, fault injection, stability and content interface testing." Applying lessons learned from this incident will lower the probability of a potential incident impacting your enterprise in the future, which is as good as it gets in cyber resilience.

[3] https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/ PIR from CrowdStrike

Root Cause Analysis

The foundation of any cybersecurity incident response process is to identify the root cause of the incident. While it often takes time and effort for analysts to dig through the log file data from multiple sources, the value comes from using the incident's root cause to consider what adjustment(s) to controls are required to reduce the probability of a reoccurrence. Enterprises that harvest lessons from cybersecurity incidents that did not impact their own enterprise demonstrate a higher level of maturity and cyber resilience. Proactive behaviors are essential to create practical initiatives from external sources and apply them through adjustments or additions to controls.

Given the growth of software supply chain compromises, which have far-reaching impacts on hundreds of enterprises today, this arena needs proactive action from CISOs.[4] As always, we should start by identifying the root cause for an incident. In the case of the Snowflake incident, Google-Mandiant determined that UNC5537 [the threat actor] harvested Snowflake credentials for customer accounts. Snowflake provides enterprise customers with data management capabilities specific to cloud accounts and services to "unite soloed data and execute diverse workloads." The malware designed by the threat actor stole Snowflake credentials from enterprise customers, of which there are currently 9,822. [5]

[4] https://www.linkedin.com/pulse/securing-future-software-supply-chain-steelcloud-ofwve/ Gartner prediction on software supply chain probability

[5] https://www.cybersecuritydive.com/news/snowflake-customer-attacks-what-we-know/719056/

The Intersection of Third-Party Risk and Identity Access Management

It's clear that Snowflake is a SaaS/PaaS offering, and access to a customer account enables access to the data stored and managed within the platform. Controls to access cloud services like Snowflake span two different cyber program capabilities: third-party governance and identity access management (IAM), defined as the digital identity controls applied to a platform's customers. When a Snowflake enterprise customer establishes service with their data management software, an individual registers an account. That same individual must also administer the registration of others in their enterprise who wish to use the data management services Snowflake provides. This is where IAM comes into play.

Often, the digital identity management process for establishing cloud accounts is not connected with the third-party governance controls for a SaaS offering, nor is it connected to the established IAM function within the enterprise. In other words, the procurement process of a cloud-based service does not enforce the digital identity controls of the purchasing enterprise as part of third-party governance. This issue leads to weak password management, which, in turn, allows threat actors to compromise credentials and obtain access to the cloud service.

SaaS account registration requires improved digital identity management controls, and herein lies the problem. IAM is not part of the third-party governance process and is therefore often missing in action when cloud accounts are registered. A cybersecurity leader attempting to apply the lesson learned from the Snowflake incident root cause analysis will discover that the third-party governance controls for digital identity management do not really exist in most enterprises. This is one dimension of the root cause of software supply chain compromise specific to third-party governance.

The second root cause is that established IAM controls at the enterprise scale were not necessarily designed for setting up SaaS accounts during the procurement process. Many enterprises with legacy technology infrastructure may not fully understand how important SaaS services (code repositories, open-source code repositories, build management software, etc.) are to software development today. Many legacy applications were developed on platforms hosted in a proprietary data center where the development environment was self-contained in that data center using mature IAM capabilities. Today, the assembly of software components happens through cloud accounts, and the IAM controls need to be designed for this cloud-first software development approach.

Conventional third-party governance controls have not substantially evolved in the past three decades even though SaaS product consumption by enterprises has exploded in growth over the past decade. Conventional controls are based on an annual risk assessment fed by a questionnaire prepared by each vendor at the request of the enterprise. The self-attestation includes questions regarding digital identity management but not specifically for cloud-based services. One of the most used questionnaires is from Shared Assessments, called the Standard Information Gathering (SIG) questionnaire. It covers 19 risk domains and can be modified for specific categories of third-party governance.[6] Enterprises must become a member of the Shared Assessments organization to use SIG, so many enterprises still use a customized questionnaire for their annual risk assessment process within their third-party governance model.

The *good* news is that most of these questionnaires are aligned with industry standards and risk management frameworks like the SOC 2 Type 2, FedRamp, or NIST CSF. The *bad* news is that an annual risk assessment based on a self-attestation is insufficient from a risk management perspective, given the explosive growth in SaaS product usage for enterprises. SaaS vendors will often choose not to respond to security related questionnaires from customers or share information about their cyber risk management practices in response to questions impacting the enterprise's ability to assess and manage risk.

Google, as a member of the Cloud Security Alliance, *does* provide enterprise customers with a SIG by incorporating the responses in their CSA STAR self-assessment artifact.[7] Other cloud service providers follow suit, offering enterprises a means for an annual risk assessment. However, can an annual risk assessment address the risks of a SaaS credential compromise? Not really.

[6] https://sharedassessments.org/about-sig/ Shared Assessments

[7] https://cloud.google.com/security/compliance/sig Google SIG

Next Generation Third-Party Governance

The risks surrounding the leakage of cloud service credentials need to be diminished through third-party governance controls with necessary digital identity management controls. It is time for enterprises to evolve third-party governance capabilities and move toward using to real-time data to detect deviations from established behavioral patterns. This new approach to third-party governance is built on a foundation of data science where vendor risk scores change based on ongoing data feeds from multiple sources. Models measure attributes daily, resulting in established patterns. When there is a significant deviation from a pattern, the models can trigger an automated workflow to manage the risk.

For example, if security intelligence sources identify leaked credentials for a third party, that vendor's risk score could change from 2.2 to 4.8 on a scale from 0-5, with 5 representing the most risk. The change in risk score is a pattern deviation and thus triggers an automated email to the vendor relationship manager and key stakeholders, like the CISO, alerting them to the change in risk score and requesting clarification. The assigned third-party governance analyst is CC'd on the automated email and tracks the follow up steps, such as factoring the supplier's response into the vendor risk score and adjusting it based on all sources of information.

If the vendor resets the exposed credentials immediately and acknowledges this step, among others, to the enterprise, then the third-party governance analyst could hypothetically change the risk score for the vendor to a 3.0 based on the supplier's response. This scenario moves the focus of third-party governance from an annual self-attestation to real-time changes in risk posture. Instead of a simple risk assessment, the new approach is an operational risk management function built on a data science foundation.

Fortunately, enterprises can choose from several vendors who currently provide near real-time data feeds across multiple dimensions. Today, enterprises typically use one set of controls for every third-party. The key is for enterprises to redesign their third-party governance model to define categories of third parties and then select appropriate controls for each category. How well the vendor conforms to the specific control requirements influences the initial vendor risk score. For example, SaaS providers should be put into a specific category with these controls:

1. Whatever security artifact they are willing to provide.
2. Attestation of the need for MFA for every privileged account.
3. An enforced policy that prevents the SaaS provider from accessing the enterprise's cloud instance.

I recommend that the vendor risk score for SaaS providers starts at a baseline of 2.0 if they comply fully with the three mandated controls for this category. Daily data feeds will drive the score up or down across multiple domains. Thus, third-party analysts do not need to chase down annual self-attestation artifacts. Instead, they can focus on when and why a risk score increases and how best to manage the risk after an event is recognized.

This approach provides a more comprehensive methodology for third-party governance incorporating IAM controls. This change in control maturity also requires education for key stakeholders, including:

- Internal auditors
- External auditors
- Regulators

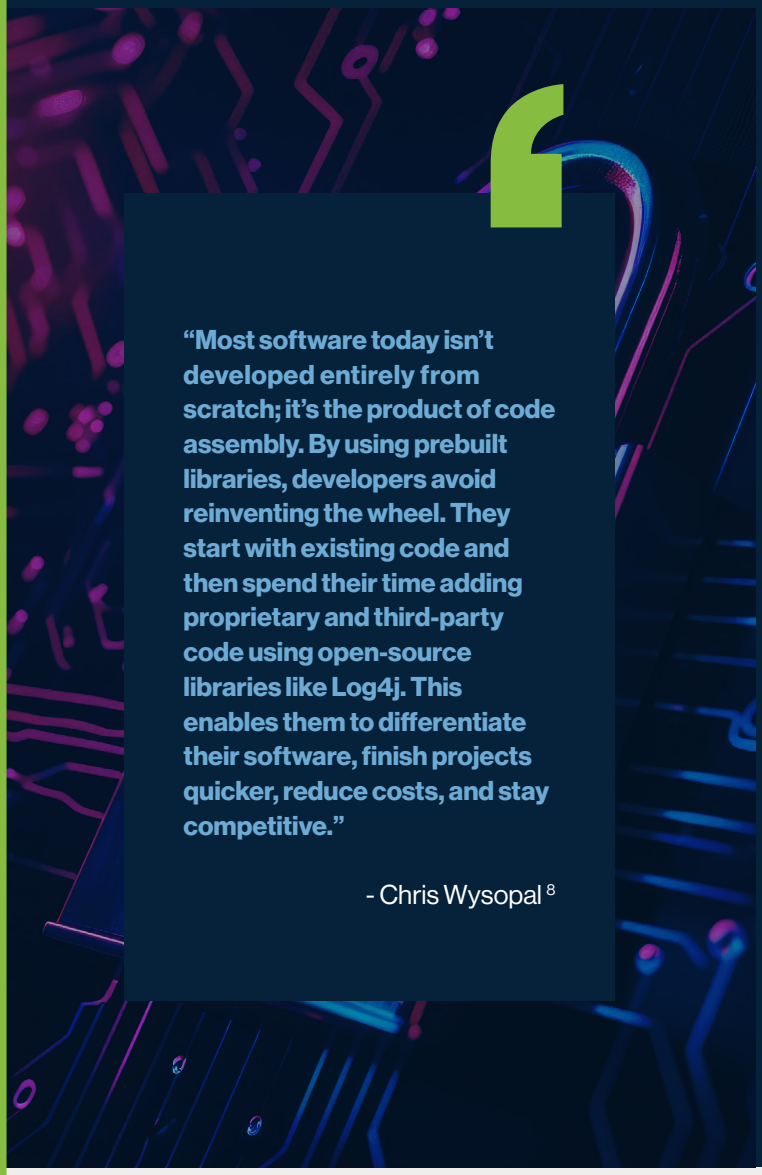
These stakeholders should not help design or implement controls, but they can and should provide their perspective on using a third-party governance model based on daily feeds and data science. At a minimum, consider giving auditors and regulators an opportunity to figure out how to adjust their review methodology and provide them with access to the vendor scoring methodology and automated workflows. They will choose what modifications are necessary for them to test control effectiveness on an ongoing basis.

This approach to third-party governance addresses both gaps in third-party controls and IAM for third parties with access to the software build process, as identified from the root cause analysis of the Snowflake breach:

1. Third-party governance for SaaS consumption by enterprises is inadequate to address the increasing demand for cloud-based software.
2. Insufficient IAM controls are being applied to cloud account provisioning and management.

These root causes stem from how software development practices have changed, moving from on-premises software development environments to the cloud-hosted SaaS services essential for software assembly today. When I developed software for enterprises 30+ years ago, I was provided with an integrated development environment. There were only two things I could do to generate cyber risk as a developer: ignore the need to use static analysis vulnerability scanning tools and promote code into a testing environment. Today, software development is done remotely using cloud services, increasing the cybersecurity risk.

Integrating software components from many different sources is the norm today and developers will seek out these resources. There are currently over twenty ways for a software developer to impact software security, from code repositories to websites featuring open-source software components, automated build tools, websites offering open source LLMs, and infrastructure as a service cloud accounts. A large majority of cybersecurity leaders do not understand this fundamental shift in cloud-first software development or the implications from a digital identity management perspective. As a result, DevOps team leaders set up up cloud accounts that need specific and established digital identity access controls that were unnecessary in the era of proprietary data centers where IAM controls were mature.



"Most software today isn't developed entirely from scratch; it's the product of code assembly. By using prebuilt libraries, developers avoid reinventing the wheel. They start with existing code and then spend their time adding proprietary and third-party code using open-source libraries like Log4j. This enables them to differentiate their software, finish projects quicker, reduce costs, and stay competitive."

- Chris Wysopal [8]

If a DevOps leader is working under a tight deadline to get a team enabled with the necessary tools to assemble code for a CI/CD automated build process, then she will do whatever it takes to configure the necessary environments. That includes making these decisions for the team:

- Determine which roles can access which environments, including cloud services, code repos, open-source websites, etc.
- Define the authentication requirements for user roles, including MFA.
- Determine the firewall protection settings for each environment.
- Identify data encryption requirements.
- Establish what additive controls are needed for privileged users, like admins, which may include authentication and monitoring.
- Apply the concept of least privilege to the access roles for the different cloud hosted services as the user population grows.
- Select the various development tools to find and fix defects before code is introduced to the build process.
- Identify the instrumentation guardrails for the automated build process.

This DevOps team leader has lots of technical skill and expertise, but limited experience applying the IAM controls essential for protecting the software supply chain, as this was previously taken care of when software was built in private data centers. This scenario represents a second root cause of software supply chain compromise. Many CISOs are unaware that technical team members make multiple security decisions every day when they establish and configure cloud service accounts. Their IAM functions are likely overwhelmed by the daily volume of cloud accounts registered by DevOps teams choosing to avoid the provisioning backlog and instead take necessary actions to enable software assembly for the enterprise.

[8] https://www.youtube.com/watch?v=y_kdElzVmng Chris Wysopal, Co-Founder Veracode, interviewed by Eleanor Dallaway, Editor Infosecurity Magazine at RSA

IAM Embedded within Third-Party Governance

CISOs who recognize the phenomena of cloud-first software development will understand the need for mature digital identity management for cloud service accounts and how it is essential for the assembly and implementation of software today.[9] Enterprises that are slow to recognize this will continue to experience the negative business impacts of software supply chain disruptions. CISOs should consider introducing their IAM team to their third-party governance team and encouraging them to work together to address the critical need to effectively onboard and control cloud accounts.

Software development with cloud accounts is essential for enterprises today to improve both software development productivity and the resilience of the software produced. This goal can only be accomplished with a mature set of digital identity management capabilities embedded within a third-party governance process that effectively manages SaaS onboarding, certification, and de-provisioning. By investing in better security today, enterprises can reap the future benefits of fewer software supply chain disruptions and, thus, lower business impact.

[9] https://www.linkedin.com/pulse/securing-future-software-supply-chain-steelcloud-ofwve/

ICIT

www.icitech.org