IMPROVING THE SECURITY OF SUPPLY CHAINS VIA AUDITING

A group proposal on how auditing vendors in a supply chain can vastly improve security, protecting not only the company, but their partners, and customers as well.

***By: Jason Rivers***

***Group members:***

Mhaliek Ferguson

Narcisse Teyiri

Hailey Thompson

Jason Rivers

***Introduction to the Problem & the Solution***

In recent years, the supply chains of businesses across the world have come under attack, from both online and offline threat actors. These brazen attacks on companies and their supply chains have increased in severity and number in the last few years, causing numerous losses to the affected businesses, their partners and consumers, as well as in very rare cases, crippling entire nations as a result. The solution to the problem supply chains face is an unbiased, clear, and professional review of their security apparatus and the practices that are in place to protect them, which is where we come in to help.

For those who may not be as knowledgeable about business terms, we’ll start with what a supply chain is. A supply chain (SC) is essentially a network of individuals, companies, and partners, as well as machines and technology that have a hand in creating a product, or the availability of a service. From the raw materials needed to be processed, to the method of how they’re created, to the transportation is all part of a supply chain. The more complex a product or service, the more links in the chain (Lutkevich, 2021). When it comes to the security of the SC, the longer an SC is, the harder it is to maintain proper security practices within it thanks to the many different aspects included.

As companies expand their operations, they need to expand their logistics and their SC as well, opening the door for threat actors to exploit vulnerabilities in their security apparatus, which has increased dramatically recently. In 2022 alone, there was a 600% increase in SC attacks according to csoonline.com (Constantin, 2022), with Gartner.com predicting that by 2025, 45% of organizations worldwide will have experienced attacks on their supply chains (Moore, 2022). These worrisome predictions require a solution to not only solve the issue, but to soothe the worries of consumers, and business owners, and that’s where we come in.

Our plan to solve this problem is to establish our own independent, external Supply Chain Audit company, which will work via contract to audit a company’s supply chain, sector by sector. An internal audit by the company itself usually focuses on where the company can improve, and track its financial performance, and may be prone to internal pressure which may influence the results. While an external audit, which carries its own concerns which we’ll discuss later, is overall more effective, is mostly immune to internal pressures on the investigation, and is much more reliable for a fair, unbiased review of SC security practices and vulnerabilities.

With this audit company, we can analyze a company’s SC sector by sector, identifying threats that could potentially arise from them. From manufacturing locations to R&D facilities, transportation, and storage sectors, and potentially even online, and brick-and-mortar storefronts, we plan to be contracted to analyze an organization’s SC link by link, and eventually, we’ll be able to audit the entire SC, something which will require significant resources, and manpower, which I will discuss later.

Each link in an SC requires a specially tailored audit, depending on the circumstances surrounding the link’s nature. You can’t audit a warehouse’s security using the same principles as an R&D facility, or an online storefront, and vice versa. We will need audit professionals, and specified teams to tackle each link, or we will need to cross-train our audit professionals to properly analyze each link, its potential weakness, and to educate them on best practices for each SC link, so the client can properly adapt to our findings, and reliable protect their SC from.

***What is an Audit Company, and Why would you need an Audit?***

Let’s start with the basics of what an audit is, the requirements for an auditor, and why many organizations rely on auditors for their security assessments. An audit is officially defined as “an official inspection of an individual or organization’s accounts, typically by an independent body.” While audits can be done internally by a company to measure their performance in certain areas, many audits, such as security audits are usually handled externally and contracted out, to avoid any sort of bias or oversights from internal investigators. The three key rules of an audit are independence, objectivity, and impartiality. Without these three guiding principles, an auditor can be unable to properly, and professionally investigate a client, and render their findings back to them for feedback. In a way, an auditor must be professionally detached from their client to do their job effectively (Bell, 2010).

In addition to having the utmost professionalism, many security audit companies require their employees to be certified auditors and obtain an audit certification in an area related to their auditing work. One of the most widely recognized auditor certifications is the Information Systems Audit and Control Association (ISACA) Certified Information Systems Auditor (CISA) certification. Many audit certifications, including CISA, require a minimum of 5 years of experience in an IT field before you’re even eligible to be certified, as well as taking a rigorous exam to make sure you understand the basics of auditing: best practices, regulations and legal requirements, and the like (Wintemute, 2023). While some companies don’t require a certification for their onboarding members and teach them in-house and on-site, generally a widely accepted certification is recommended by audit companies, and by clients alike.

Many audit certifications vary slightly, but the general basis is the same as for the CISA. There are 5 main domains that potential auditors are tested for, which they will be using practically in their role as an auditor. Those domains are as per the CISA exam outline:

* ***Information Systems Auditing Process:*** Includes Audit Standards, Guidelines and Code of Ethics, the different types of audits, and assessments, evidence collecting, and Quality Assurance
* ***Governance and Management of IT:*** Includes IT Governance, Strategy, Frameworks, Policies, and Procedures, Organizational Structure, and risk management. Laws, regulations, Industry Standards, and compliance, as well as resource management.
* ***Information Systems Acquisition, Development, and Implementation:*** Goes over project management, system development, and control design, as well as system migration, infrastructure deployment, and Data Conversion.
* ***Information Systems Operations and Business Resilience:*** Covers IT components, asset management, scheduling of processes, plus System, Incident Response, Configuration\Patch, and Database management. Also delves into System resiliency, and emergency recovery/backup plans in the event of a worst-case scenario befalling the client.
* ***Protection of Information Assets:*** The largest section covered in CISA, including IT Security Frameworks, guidelines, and standards, privacy principles, Access management, and Network/End-Point Security and cryptography standards and implementation. Also, security awareness of employees, training programs, attack methods that could be used against the client network, incidence response, evidence gathering, and producing findings.

These domains cover a large part of the skills an auditor will be utilizing, as well as what they will be investigating, and reporting back to the client on. There are several other “supporting tasks” they are tested on, but they mainly serve to reinforce what the exam goes over, as well as what they’ll be utilizing in the field.

Now that we’ve established what an audit is, and what an auditor requires to perform their job, how is an audit performed? Audits are generally done utilizing interdisciplinarity, meaning that auditors investigate many different aspects of a company’s security, culture, and general handling of different aspects. An audit can involve traditional auditing of financial and business aspects, or physical security of brick-and-mortar locations, information systems and/or information security, behaviors, training, and security knowledge of employees and partners, general IT aspects, and in recent years, cloud computing and storage aspects of an organization. In addition to audits mostly being of an interdisciplinary nature, many audits are unique in the way that each investigation has to be tailored to the client’s supply chain layout, IT infrastructure, and other variables, meaning that one of the biggest challenges for an audit team is to outline an investigation plan based on the client’s request, and the client’s organizational aspects and layout (Lo & Marchand, 2004).

Despite the rigorous certification tests and everything that involves an audit, the process of performing one is fairly simple. To begin with, the contracted auditor(s) will meet with the leadership of the client organization and discuss the planned audit, including the scope of the audit and objectives, as well as risks involved, and potential roadblocks to meeting those objectives. After everything is discussed, and goals are set, the auditor firm will put together a team to perform the task, with members best suited based on the scope and goals set by the client. Next, the audit team gathers documentation, data, and information pertaining to the audit, such as reports, policies, organizational practices, procedures and manuals, as well as IT infrastructure, database information, and information about the supply chain partners and vendors. (Judge, 2023). Some audits of a more IT-focused nature can even involve penetration testing (Easttom, 2017), or a phishing experiment and anonymous survey to test employees on best practices versus a social engineering attack (Nohlberg, 2005).

Next, after the data is gathered, it’s all analyzed, and reports are constructed based on the results of the documentation, and (if applicable) the pen tests, and social engineering tests. The audit team meets with the client organization’s leadership and reports on findings: where the supply chain is strongest and weakest, and offers recommendations to solve those weaknesses, emphasizing the benefits of these proposed changes. After discussing the findings with the clients, an audit team will usually also have a hand in creating an action plan for the organization to tackle the results of the audit’s results. This can be anything from changes to protocols and procedures to altering the supply chain’s IT infrastructure or retraining employees on best practices, and security procedures. Finally, the client and audit team set up a follow-up plan to track the progress of the changes, monitor the company’s supply chain performance as a result of the changes, and schedule a follow-up audit to again analyze the company’s supply chain based on changes made. Feedback is also collected from clients to review the audit team’s performance, analysis skill, and suggested changes for their own future developmental use (Judge, 2023).

Now that we’ve firmly discussed auditors, their professional requirements and what an SC audit consists of, we can finally talk about why SC audits are such an important requirement for organizations. The most obvious reason is simply growth and improvement. An audit is done to analyze a company’s performance as we’ve discussed, highlighting its strengths and weaknesses, suggesting changes that could help take a company just a little further with its SC and resources, and allowing resources freed up from optimizing its SC security to be put elsewhere within the organization, leading to growth. One of the biggest things that saves resources is the prevention of SC disruptions, which an audit can help with.

As we’ve discussed, an audit’s purpose is essentially threefold: to assess your SC security strengths and weaknesses, to recognize the risks associated with different factors such as partners, vendors, or practices, and finally to remediate them to either completely negate those risks or reduce them to a suitable level. Risk negation lowers the threat of a vulnerability in an SC being leveraged, which in turn prevents attacks, and reduces SC losses. Even something as simple as petty theft from an employee, or an external criminal can contribute to losses via SC vulnerabilities. In 2007, the FBI reported that each year, between $10 and $30 billion per year are lost due theft of cargo thanks to vulnerabilities in SC transportation sectors (Anderson, 2010).

Even outside of basic theft, risks of cyber-attacks on SCs are a dangerous, ever-growing threat, which only seems to grow as time goes on. According to Statista.com, in the US in 2022 alone, the number of SC cyber-attack victims soared to 1743 affected entities, compared to 2021’s 521 (Petrosyan, 2023). Each attack on the SC leads to losses from successful attacks, and potentially disruptions caused by unsuccessful attacks and the fallout from both. Vulnerabilities in SC IT infrastructure are leveraged, allowing for threat actors to exploit weaknesses that an audit may have found. A common IT-related weakness in SC involves database access, and information sharing between organizations, and vendors. In more infamous attacks, even the database of vendors themselves have been leveraged to successfully spread malware to clients, compromising their systems; we’ll talk more about this later. For now, let’s talk about the basic risk posed to SC security by vendor vulnerabilities.

It’s a matter of fact that the more complex an organization’s supply chain, the harder it is to properly secure, and that becomes much harder as you include business partners and vendors. With how intimately involved some vendors are in an SC, it’s natural that a variety of information and software will need to be shared between them, which is where some hackers identify weaknesses. Attackers have many ways they can leverage weaknesses from an SC vendor, including insider assistance either intentionally, or from social engineering (Urciuoli et al. 2014), to company device theft (Urciuoli et al. 2013), and simple software glitches in their systems which can be exploited. An organization’s security is only as strong as the weakest link. Unfortunately, vendors and SC partners tend to be the weakest link in the security of many SCs.

The importance of an SC audit is that it can help not only the direct client but vendors as well. An audit can help identify weaknesses in client-vendor data sharing by investigating organization databases, protocols and practices revolving around data-sharing, authenticating vendor employees and in many cases, auditing vendors themselves. By auditing vendors, and improving their own security, as well as any direct links an organization has to a vendor that could be leveraged, you can bolster SC security even further (Pandey et al., 2020). The impartiality of an independent audit firm can ensure that client and vendor information remains confidential and that security in any involved organizations improves to protect all parties involved in an organization’s SC. One exploited vulnerability in a vendor or organization’s SC could have disastrous consequences that ripple throughout their SC, damaging vendors, and client organizations alike unless security is maintained by a 3rd party audit firm. Historically, those consequences have even crippled nations.

In 2017, a particularly nasty “wiper” ransomware was let loose on Ukraine, and the world by Russian-backed hackers, which essentially crippled the country for a time, and it had incredibly wide-reaching effects across the world. A basic overview of the whole affair is essentially that Russian-backed hackers broke into the servers of a small Ukrainian software vendor, Linkos Group who created and maintained a widely used accounting software called M.E.Doc. This software was used in essentially every facet of Ukrainian business, from governmental to medical, financial, and even education and individual devices. What the hackers did was they uploaded an infected update to the vendor which began to send the malicious update out to clients across the country, which would then begin to lock out devices, falsely demand a ransom, and wipe all information from the device and then spread to other devices on the same network (Robinson et al., 2022). Because M.E. Doc was a financial software vendor involved in the SC of many Ukrainian and international organizations, the entire country was brought to a financial standstill until this was resolved.

Given that Linkos Group is a “small, family-run Ukrainian software house” (Robinson et al., 2022), it’s likely that proper security auditing wasn’t performed on their organization, or by many of the organizations who were clients of their SC. It’s difficult to find any evidence of whether Linkos Group did or did not undergo yearly security audits, but running under the assumption that they didn’t, an audit could have helped to prevent the server breach that led to this situation in the first place. In fact, this incident spawned a flurry of discussions among organizations worldwide about and emphasizing the need for yearly supply chain and security auditing to prevent this very same situation from happening again.

Independent audit firms are important for assessing the security, protocols, and practices in place in an organization. They can help identify strengths and weaknesses, and even discover new areas of vulnerability thanks to their impartiality, and specialized investigations. A simple yearly audit alone can save not only potentially hundreds of thousands in losses but also prevent an organization from being the victim of an SC attack, a possibility which unfortunately grows every single year.

***How Our Innovation Relates to Interdisciplinarity***

One of the most important things about auditing is how interdisciplinary it is in its nature. It combines multiple different schools of thought from risk management, analysis, forensics, and business, as well as the skills it involves like communication, IT knowledge, teamwork, and goal-oriented objectives. All of these and more are key to an individual auditor’s success, and the success of an entire firm. We’ll come back to this later, but for now let’s discuss the problems that security audits solve, and how they too are interdisciplinary.

As we’ve discussed, threats facing organization’s SCs are varied in nature. All in all, they pose a threat to the overall business and economics of the organization itself, the business partners, and shareholders who invest in the organization, the consumers who rely on it for the goods and services it produces, and finally (and most importantly in my opinion) the people who rely on the organization for employment. Any disruption inflicted on an SC can result in losses which cause layoffs or firings and can negatively affect all parties involved in a business. While you can’t predict every single SC disruption, you can control and reduce the chance of a security issue happening that causes one. Risk reduction and risk assessment are 2 disciplines we learn about at ODU that are huge in businesses, and auditing is key to both disciplines.

Another issue that security auditing can help with is streamlining developments in security areas, from IT to employee training, best practices, and information sharing between business partners and vendors, both IT and non-IT related. The feedback an audit can provide can be key to guiding and making changes to protocols, and practices in place at an organization that aren’t as efficient as other options, or outright contribute to security risks. The biggest weakness often identified in an organization’s security is the human element, and in the same vein, the biggest security threat often identified in SC is vendors. An audit can help make changes to how and what you train employees and ensure that they utilize their training to prevent security incidents. Concurrently, audit feedback can also make changes to how much information, and what information vendors are privy to. Communication is key in business, however communicating too much information, or information that’s too confidential to a vendor is a threat not only due to leaks but also if they face their own security breaches as well.

Now that we’ve established interdisciplinary problems that auditing solves, we’ll explain how our solution is interdisciplinary. As we discussed before, auditing involves multiple schools of thought and skills. An audit almost always covers several different topics, meaning either individual auditors need sufficient knowledge of different schools of thought, or that an audit team needs to be made up of individuals who specialize in each required area for a specific audit request. Some of the biggest ones are, as we’ve discussed, business, communication, training, and data analysis.

Key to their job, auditors need to analyze vast amounts of data and give feedback on it to clients in order to guide changes and development post-feedback. Then need to develop ways that a client can make changes to their business model, or aspects of it where faults have been discovered. They also need to have knowledge pertaining to employee training, and utilizing their knowledge of best practices, and protocols to make necessary changes to a client’s in-place security measures. Finally, they need to be able to communicate this information back clearly and concisely to a client so that changes can be made, and the necessary steps can be taken to begin making those changes to a client’s organization to improve its SC security. In the same school of thought, they also regularly schedule follow-up audits, or appointments to check up on any changes being made per their recommendations.

***How to Know if our Innovation is Effective***

The biggest question we’ve had so far actually pertains to this topic: how will we be able to identify if our innovation is effective? The answer to that is that our clients who we audit will notice increases in efficiency over time, a reduction in losses due to theft and security-based disruptions, and overall reductions in internal risk assessments. If our audit comes back with sufficient evidence of current SC security underperformance, and we communicate that to a client who uses it to improve, I see that as our innovation being used effectively.

When we audit a client, we need to be able to identify weaknesses in their security apparatus, if any are apparent, and analyze the data we collect to sufficiently measure their security. If we come up with nothing, that might be a sign that we weren’t rigorous enough in our investigation, or that our methods of measuring a client’s security, practices, and protocols are wrong, and we need to make changes to be more effective. If we aren’t able to sufficiently identify and communicate feedback, our innovation will suffer as will our clients.

Arguably the biggest way our innovation will be effective is in how we develop, organize, and follow up on our feedback, and suggested changes to a client’s SC security infrastructure. If a client makes changes as per our suggestion, then sees a reduction of losses or more efficiency in their SC security, I see this as a win. On the other hand, if they make changes, and see either an increase, or no change in losses or even worse, experience a lapse in security in an area where we suggested a change, I see this as a major issue, and something we will need to address. Overall, the reason for an audit is to measure the strengths and weaknesses of an organization in the area it’s being audited. If the results of an audit can make a positive change to an organization, I see this as proof that our innovation works.

***How to Make Our Innovation a Reality***

We discussed before that many audit firms require members of their audit teams to be certified auditors, requiring not only a baseline of experience (5 years in our example), but to undergo a rigorous knowledge exam as well. I believe that our firm should follow suit and require all members of our audit team(s) to be certified, with sufficient experience in either IT, business, or risk management fields to contribute to our teams. If we aren’t completely confident in our own team members, how can we expect our clients to be confident in them, or us for that matter? Another matter is confidentiality pertaining to the information we analyze on behalf of clients.

A common threat associated with an audit team analyzing client information is that the information given will be leaked, and otherwise used against them, which is where non-disclosure agreements (NDAs) come in. Each of the members of our audit teams will be expected and required to sign clients’ NDAs before being given access to each client’s information. We will also compromise with clients on how, when, and where we use their information; an example is if they wish for us to only analyze information on their property, using their own devices, we will try and work with them regarding these parameters. Any member of our audit teams who violated an NDA, or violated a client’s information handling parameters will immediately be terminated. We need 100% trust between us and clients otherwise we can’t do our duty as well as we need to.

Aside from recruiting and enforcing standards on our new hires and members of our teams, we’ll need to secure funding to get started, identify competition in the local market, and get our name out to potential clients. First, we need to create a team of professional auditors, and lay the foundation before we can do anything. Without proving to investors and banks that we have the potential due to this, we won’t get far. In addition to that, we’ll need an Employer Identification Number and a Tax ID Number. After we secure the basic business requirements and initial funding, we can start conducting research into potential clients, analyzing local competitors, and advertising ourselves to clients. We need to start relatively small; with a small team, we’ll likely only be able to handle one client at a time to avoid stretching ourselves too thin.

With some of the initial funding, we can use it to secure hardware and software for our initial audit team. We likely won’t need to lease an official in-person office, we can use a work-from-home model starting out to reduce costs and have our team members meet up in person for client meetings. We’ll also need to recruit someone to handle the firm’s accounting, and when we start expanding our operations, we’ll need a human resources member to handle employee concerns and expand our human elements. Finally, we need to identify any sort of legal roadblocks, or legal concerns that might cause us issues down the line. The biggest ones that pop out are how we handle client information, NDA’s, employee information, and basic business legality. For all of this, we can hire a lawyer to assist us with the legal aspects of business handling and help us word our employee and client contracts.

Overall, I think our innovation requirements are fairly standard for a business. The biggest challenge for us will be earning and finding members with proper experience and certifications to do the job. After that, securing funds, investors, and initial clients will be key. If we can do our job well, and advertise via word of mouth, we should be able to get a foothold versus local competition like LRQA, or Sera-Brynn. After that, we just need to focus on doing our job, and doing what our innovation was made to do.

***What are Our Next Steps?***

Finally, we can discuss our next steps. Our direct next step to establish this innovation is for us to acquire experience in IT, business, and communication, as well as the certifications we discussed earlier. Without these, we can’t even proceed to the foundational steps required for this innovation. The investment from us is significant, but we believe that the payout from it will be well worth the wait, and the resources we spend on it.

Overall, I think I learned a lot from this project. I have a friend who works for the government as an auditor, and from the way he describes it, it’s mostly a bunch of meetings with clients, and with his auditor company; very boring, long days, but a lot of downtime. I learned there’s more to auditing than meets the eye. It involved a lot of experience, knowledge of protocols, best practices, legal requirements, and basic knowledge of various areas. It also involves a lot of legality when it comes to sharing information, handling it, and ultimately protecting client data from not only bad actors, but their own business partners or vendors, not necessarily out of malicious intent, but for both of their own good.

One of the most prolific best practices currently that auditing can lead to is a “zero trust model” where no specific members, partner, or vendor associated with an organization is trusted, and everyone is suspected. If you plan for everyone to be a suspect of a leak, breach, or SC disruption, you can actively plan to counter it, but I’m getting off-topic.

Finally, what I would have done differently is I would have probably would have focused the audit on smaller businesses specifically for the time being. While smaller businesses are less likely to be hit, they are still susceptible to supply chain attacks, so one disruption could cause irreputable damage to a small business. Overall, however, I love the innovation we chose.

***Works Cited:***

Bell, T. J. (2010, June). *The Social Psychology of IT Security Auditing From the Auditee’s Vantage Point: Avoiding Cognitive Dissonance*. egloos.com. <http://pds20.egloos.com/pds/201009/09/02/jpdf1003-the-social-psychology.pdf>

Constantin, L. (2022, October 19). *Supply chain attacks increased over 600% this year and companies are falling behind*. CSO Online. <https://www.csoonline.com/article/573925/supply-chain-attacks-increased-over-600-this-year-and-companies-are-falling-behind.html>

E. C. Lo and M. Marchand, "Security audit: a case study [information systems]," Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513), Niagara Falls, ON, Canada, 2004, pp. 193-196 Vol.1, doi: 10.1109/CCECE.2004.1344989 <https://ieeexplore.ieee.org/abstract/document/1344989>

Easttom, C. (2017). 1. Introduction to Penetration Testing. In *Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits* (pp. 9–19). essay, Pearson.

Judge, J. (2023, October 19). *How to perform a Supply Chain Audit: Key steps & best practices*. certaintysoftware.com. <https://www.certaintysoftware.com/how-to-perform-a-supply-chain-audit/>

Moore, S. (2022, April 13). *Gartner top security and risk trends in 2022*. Gartner. <https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022>

Nohlberg, M. (2005). Social Engineering Audits Using Anonymous Surveys: Conning the Users in Order to Know if They Can Be Conned. In Proceedings of the 4th Security Conference, Las Vegas. Retrieved from <https://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-25668>

Lutkevich, B. (2021b, June 2). *What is a supply chain? - definition, models and best practices*. WhatIs.com. <https://www.techtarget.com/whatis/definition/supply-chain>

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020, January 17). *Cyber security risks in globalized supply chains: Conceptual Framework*. Journal of Global Operations and Strategic Sourcing. <https://www.emerald.com/insight/content/doi/10.1108/JGOSS-05-2019-0042/full/html#sec013>

Petrosyan, A. (2023, January). *Annual number of Supply Chain Cyber attacks U.S. 2022*. Statista. <https://www.statista.com/statistics/1367208/us-annual-number-of-entities-impacted-supply-chain-attacks/>

Robinson, A., Corcoran, C., & Waldo, J. (2022, May 16). *New risks in ransomware: Supply chain attacks and cryptocurrency*. Harvard Library. <https://dash.harvard.edu/bitstream/handle/1/37373233/Paper_Waldo_Ransomware_FINAL.pdf?sequence=1>

[Urciuoli, L.](https://www.emerald.com/insight/search?q=Luca%20Urciuoli), [Mohanty, S.](https://www.emerald.com/insight/search?q=Sangeeta%20Mohanty), [Hintsa, J.](https://www.emerald.com/insight/search?q=Juha%20Hintsa) and [Gerine Boekesteijn, E.](https://www.emerald.com/insight/search?q=Else%20Gerine%20Boekesteijn) (2014), "The resilience of energy supply chains: a multiple case study approach on oil and gas supply chains to Europe", [*Supply Chain Management*](https://www.emerald.com/insight/publication/issn/1359-8546), Vol. 19 No. 1, pp. 46-63. <https://doi.org/10.1108/SCM-09-2012-0307>

Urciuoli, L., Männistö, T., Hintsa, J. and Khan, T. (2013), “Supply chain cyber security–potential threats”, Information and Security: An International Journal, Vol. 29 No. 1, pp. 51-68.

Wintemute, D. (2023, October 5). *How to become a security auditor*. CyberDegrees.org. <https://www.cyberdegrees.org/careers/security-auditor/how-to-become/>