SPOTLIGHT / SUPPLY CHAIN RISK

What Risks are Hiding in Your Supply Chain?

If you were to ask 100 supply chain executives what is the biggest risk facing multinational corporations today, you would probably get at least 100 different answers. Knee-jerk responses would likely include natural disasters, supply/demand imbalance, cybersecurity, global economic instability, etc. While these are, indeed, all critical risks, the most dangerous and potentially destructive risks are the ones you underestimate.

The World Economic Forum's (WEF) 2016 Global Risks Report finds that supply chain vulnerability is on the rise, and the interconnections between risks are becoming stronger. WEF calls upon both the public and private sectors to embrace a "resilience imperative," a culture of integrated risk management and multi-stakeholder partnerships.

The most dangerous and potentially destructive risks are the ones you underestimate.

With the list of potential risks – internal/external, upstream/downstream – growing almost daily (a Rand International report (http://www.rand.org/content/dam/rand/pubs/documented_briefings/DB600/DB649/RAND_DB649.pdf) puts the number at nearly 150), there is "an urgent necessity to find new avenues and more opportunities to mitigate, adapt to and build resilience against global risks and threats through collaboration among different stakeholders," according to the World Economic Forum's (WEF) Global Risks Report 2016.

Many high-tech companies, like ON Semiconductor, have long recognized that having a strong risk mitigation strategy can be a valuable asset and a competitive differentiator. They also understand that true resilience is not something that can be accomplished in a vacuum. One aspect that sets ON Semiconductor's risk management program apart is its deep collaboration with its insurer FM Global.

"It may seem a little illogical to go to your insurance company and show them everything, all the risks, all the dirty laundry," said Brent Wilson, senior vice president of global supply chain operations and procurement for ON Semiconductor. "But, visibility is the key to mitigating any risk. Being fully transparent with FM Global about our operations, the products that flow through our factories, our customers, etc., gives them the visibility they need to help us identify exposures."

Brent Wilson
ON Semiconductor

Each year ON Semiconductor and FM Global "do deep dives in different sites," and once the risks are identified, ON Semiconductor works with FM Global to develop mitigation strategies. "The deal is, when we fix things, they lower our score; and the lower the score, the lower the insurance premiums."

The program started with just one factory, Wilson explained, but has since been extended to all of ON Semiconductor's wafer fabs and assembly and test sites. "They are not just actuaries, but also engineers, so they understand the systems and what we are trying to accomplish. At the same time, they look at risk differently than we do and they quantify it differently, so they are able to give us a different perspective on some of those risks."

Wilson admits that collaborating with FM Global was a bit of a leap of faith in the beginning, but with all the consolidation that is going on in the semiconductor sector, he says companies need to approach risk management with more creativity. "We are seeing more single strands in the supply chain, due to consolidation. Even if our suppliers are not directly impacted by an event, we are seeing a cascading effect that puts stress on the entire supply ecosystem."

With all the consolidation that is going on in the semiconductor sector, companies need to approach risk management with more creativity.

Next, we will take a closer look at three specific risks that may not be the most likely, or most impactful, but definitely should not be underestimated. These risks – water scarcity, supply chain fraud and malicious counterfeits – represent both emerging and persistent threats to the electronics supply chain, which industry insiders believe may escalate quickly as the global supply chain grows ever-more reliant on goods and services from emerging markets and under-developed economies.

New Security Vulnerabilities Uncovered in IC Supply Chain

In 2012, a U.S. Senate Armed Services Committee investigation (http://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts) found more than one million suspected counterfeit electronic parts within the Department of Defense supply chain. The functionality and reliability of these parts, which may have been harvested from e-waste, reverse engineered, produced by illegal manufacturing overruns, or a variety of other means, is at best, unpredictable, at worst, non-existent. Among the defense systems in which these parts were discovered, included Traffic Alert and Collision Avoidance Systems (TCAS) for Global Hawk drones, Excalibur (an extended range artillery projectile), the Navy Integrated Submarine Imaging System and the Army Stryker Mobile Gun.

Now imagine, that instead of being shoddily remarked defects or reclaimed e-waste, these one million parts were purposely altered at some point during the IC design, fabrication or manufacturing processes, to include malicious functionality, such as kill switches, viruses or backdoors that could leak sensitive information or enable an attacker to seize system control. Add IoT connectivity into the mix, and suddenly, the attack surface becomes almost limitless.

"Hardware is the root of trust in electronics devices, it must be secure by design."

Jon Boyens, NIST, US Dept. of Commerce

This is the threat that is emerging in the electronics supply chain, according to Jon Boyens, program manager, cyber SCRM, National Institute of Standards and Technology (NIST) for the U.S. Department of Commerce. "Hardware is the root of trust in electronics devices, it must be secure by design. The problem we have with new technology is that when it is being built, security is not being built in, it is bolted on after the fact which makes it more difficult to produce and less effective."

Just a few years ago, the hardware malware threat was considered more theoretical than practical, and though confirmed reports of systems failures due to malicious hardware tampering are rare, the feasibility of this threat is growing by orders of magnitude. Just last month, researchers from the University of Michigan demonstrated the vulnerability of an integrated circuit to digital-layer design time attacks, as well as corruption of analog circuits at the time of chip fabrication. The report, A2: Analog Malicious Hardware (http://static1.1.sqspcdn.com/static/f/543048/26931843/1464016046717/A2_SP_2016.pdf?token=N4pJSSoqL4kE4V4JXpTwx7qDRX4%253D), concluded that one gate was all an attacker needs to compromise the security of an integrated circuit and gain full access to a system's operating system – one gate amid millions on the typical IC. Detecting this chip-level tampering is analogous to finding a needle in a haystack of needles, according to a 2015 paper entitled Performance analysis of Hardware Trojan detection methods (http://injoit.org/index.php/j1/article/viewFile/195/152) in the International Journal of Open Information Technologies.

Researchers from the University of Michigan demonstrated the vulnerability of an IC to both digital-layer design time attacks and analog circuit corruption during chip fabrication.

Since the vast majority of the safeguards within the supply chain are predicated on the assumption that profit is the end game of "counterfeiters," detection strategies focus on the

identification of parts that have been reclaimed, remarked, re-engineered or otherwise fraudulently represented. But, when the motivation is widespread economic disruption or breaching national security defense systems, the corruption mechanism is typically more sophisticated. Hardware trojans do not typically impede the normal functioning of the chip until they are triggered, so, this kind of tampering is unlikely to be detected via standard inspection and testing protocols. In fact, "even the fastest automated testing methods would take many years to exhaustively test everything that a modern large chip can do," according to a paper by John Villasenor, senior fellow in Governance Studies and the Center for Technology Innovation at the Brookings Institute (http://www.brookings.edu/~/media/research/files/papers/2013/11/4%20securing%20electronics%20supply%20chain%20against%20intentionally%20compromised%20hardware%20villasenor/compromised%20by%20design%20securing%20the%20defense%20electronics%20supply%20chain.pdf).

What does this mean for supply chain executives? While in the past attackers labored to exploit security gaps that might exist in corporate or national defense IT systems, today the gaps they are exploiting are in the integrity and security of the supply chain. Therefore, as the threat landscape evolves, it is essential for an effective supply chain security strategy to proactively minimize exposures throughout the entire lifecycle – from cradle (secure IC design, fabrication and manufacturing) to grave (ethical e-waste disposal) and everything in between. It must also reflect the reality that most electronic systems are built with chips that were designed and manufactured outside the OEM's home market – unless that OEM is based in China or one of the other popular regions for off-shore wafer fabrication.

In the past, attackers labored to exploit security gaps in IT systems, today the gaps they are exploiting are in the integrity and security of the supply chain.

While this may sound like a daunting, and expensive, undertaking, many of an organization's existing tools for managing supply chain risks involving quality, integrity, security and continuity can also be useful in defense against cyber risks, said Boyens.

For example, the quality assurance mechanisms and audits many companies use to assess and manage vendor performance can easily be amended to integrate cyber security criteria as well. Boyens recommends that supply chain professionals confer with their corporate IT security experts to add cyber risk to the vendor selection and performance reviews.

Similarly, according to Boyens's Integrating Cybersecurity Into Supply Chain Risk Management (https://www.rsaconference.com/writable/presentations/file_upload/grc-w03_integrating_cybersecurity_into_supply_chain_risk_management.pdf) presentation at the 2016 RSA Conference, track and trace tools used gather information on parts and materials to ensure quality, integrity and to backstop warranties can provide valuable visibility by part, supplier and production process down the supply chain. Providing a complete pedigree for manufactured products, for example, may give organizations the capability to distinguish between design flaws and deliberate defects. "Knowing the provenance, or who has touched the product or service along the supply chain route, is the holy grail for supply chain security," Boyens said.

While there is growing awareness of the risk of hardware tampering, when companies are making strategic decisions based on the golden triangle of cost, performance, and schedule, cost and schedule often outweigh the performance/security aspects, Boyens explained.

These choices may prove more than just costly, but deadly. "Chip design represents a gaping and exploitable hole in the current approach to supply chain security," Villasenor wrote in his paper Compromised By Design? Securing the Defense Electronics Supply Chain (http://www.brookings.edu/~/media/research/files/papers/2013/11/4%20securing%20electronics%20supply%20chain%20against%20intentionally%20compromised%20hardware%20villasenor/compromised%20by%20design%20securing%20the%20defense%20electronics%20supply%20chain.pdf). "Too often, we wait for catastrophe to spur change," he concluded. "As there has not yet been a string of publicly disclosed examples of defense hardware with malicious design alterations, it is hard to spur interest in investing significant effort to address the inevitability of intentionally compromised hardware. But given the critical role of chips in nearly every defense system, there are good reasons to be proactive as opposed to purely reactive with respect to hardware cybersecurity."

What Happens When the Well Runs Dry? Implications of Water Scarcity Risk in the Supply Chain

With recent reports of deadly flash floods (http://www.cnn.com/2016/06/28/us/west-virginia-flooding-weather/) ravaging parts of the U.S. Southeast, and global El Nino Southern Oscillation (ENSO) (http://thediplomat.com/2016/07/torrential-rains-wreak-havoc-in-southern-china/) weather patterns driving torrential rains and flooding in southern China, it may be hard for many organizations to consider water scarcity a significant supply chain risk, but, regions across the globe are, in fact, facing a staggering supply/demand imbalance.

The World Economic Forum's (WEF) 2016 Global Risk Report (http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf) identified the lack of safe drinking water (https://www.weforum.org/reports/the-global-risks-report-2016/) as the most serious risk facing the global community over the next 10 years. WEF also projects that demand for potable water will exceed sustainable supply by 40 percent by 2030. The United Nations (UN) Water (http://www.un.org/waterforlifedecade/scarcity.shtml) policy committee further predicts that by 2025, 1.8 billion people will be living in countries or regions with absolute water scarcity, and a full two-thirds of the world's population could live under "water stressed" conditions. As a result, the CDP Global Water Report 2015 (https://www.cdp.net/en-US/Pages/events/2015/water/global-water-report-2015.aspx) claims that water security may be "the defining environmental issue of the 21st century."

The lack of safe drinking water is the most serious risk facing the global community over the next 10 years.

Though there is, in theory, enough freshwater on the planet to sustain seven billion people, according to the UN, it is "distributed unevenly and too much of it is wasted, polluted and unsustainably managed." This is, actually, good news, because it means that improvements in both national and corporate water governance can make a true difference in mitigating this environmental crisis.

For members of the electronics supply chain water stewardship represents both a practical imperative to mitigate risk and an opportunity to promote strong corporate citizenship.

Water stewardship represents both a practical imperative to mitigate risk and an opportunity to promote strong corporate citizenship.

For example, to demonstrate that it values environmental sustainability, ON Semiconductor's water conservation efforts included a commitment to reducing its operational water consumption by 5 percent. The company also supported ongoing sustainability programs that include reusing rinse water for HVAC systems and reducing water flow during equipment idle periods.

Still, water scarcity wasn't an urgent priority for ON Semiconductor, until climate change in regions where it had two major facilities prompted local governments to threaten water restrictions. The sites represent about 30 percent of the company's total corporate revenue, explained ON Semiconductor's Brent Wilson, so time was definitely of the essence. ON Semiconductor immediately activated a global crisis team that included procurement personnel and water experts from several facilities. Though the crisis passed without the need for water rationing, the experience revealed some significant exposures in the operations.

Water scarcity wasn't an urgent priority for ON Semiconductor until two major facilities faced water restrictions.

"We knew this was an issue that could come back and, if we didn't make some changes, it would be very difficult for us to continue operations during a water shortage," Wilson said. "A lot of companies will get through a crisis like this and they are just happy that they can move on. But, our process is to go back after the dust settles and do a deep dive to see what we could have done better, what are things that still need attention, what can we do so that we are better prepared next time."

In response to this post-event investigation, ON Semiconductor developed strategies to enable them to only run key bottlenecks if water supplies are low. To try to keep water flowing despite local conditions, ON Semiconductor established some redundancies in the fire safety systems at

Fact$_2$0

One semiconductor manufacturing plant uses between 2 to 4 million gallons of ultrapure water per day – the equivalent of a city of 40,000-50,000 people.

Source: Dr. Farhang Shadman, director of the Engineering Research Center for Environmentally Benign Semiconductor Manufacturing.

a number of at-risk facilities to enable them to store large quantities of water.

"We have a whole blueprint now, so if/when this happens again, we have a strong plan," said Wilson. "And, the facilities team owns part of it, the procurement team owns part of it, the local factory GM owns part of it – we all have our parts to play."

Because the bulk of many high tech organization's water footprint is tied to the manufacturing activities of its suppliers, some may have a "false sense of security about water risk exposure," according to a report from the Pacific Institute, Water Scarcity & Climate Change: Growing Risks for Businesses & Investors. The report cautions companies to consider not only the financial implications of water scarcity – lower productivity, operating disruptions, increased infrastructure and maintenance costs, etc. – but the potential brand impacts as the manufacturer's water needs come into direct competition with local populations. "Large water withdrawals can result in reputational damage in regions where water is scarce and/or local populations lack access to safe and affordable drinking water."

Whether the impacts of water shortage are direct or indirect, "all businesses will be adversely impacted to some extent by physical, regulatory, reputational or litigation risks," a white paper entitled Is Water the New Oil? from Zurich Insurance concluded. "Risk managers and business leaders, who have long relied on a continued supply of water, need to revise their risk management and long-term planning processes to include the reality of water shortage."

Supply Chain Forensics: Using Big Data to Identify and Fight Fraud

And, finally, we have the risk that dare not speak its name – supply chain fraud. Despite reports from the Association of Certified Fraud Examiners (ACFE) (http://www.acfe.com/press-release.aspx?id=4294973129) that the typical organization loses five percent of its revenues each year to fraud – which equates to nearly US$3.7 trillion global loss annually – supply chain fraud remains significantly under scrutinized within many companies, according to Mark Pearson, principal in the Forensics & Investigations practice of Deloitte Financial Advisory Services LLP.

A recent Deloitte Advisory poll found that 40 percent of companies believe fraud is likely or extremely likely to occur across their organization and 30 percent said their companies had experienced supply chain fraud, waste or abuse in the past year. Yet, 26.8 percent report that they currently have no program in place to prevent and detect those risks and only 29.3 percent use analytics to mitigate supply chain fraud and financial risks.

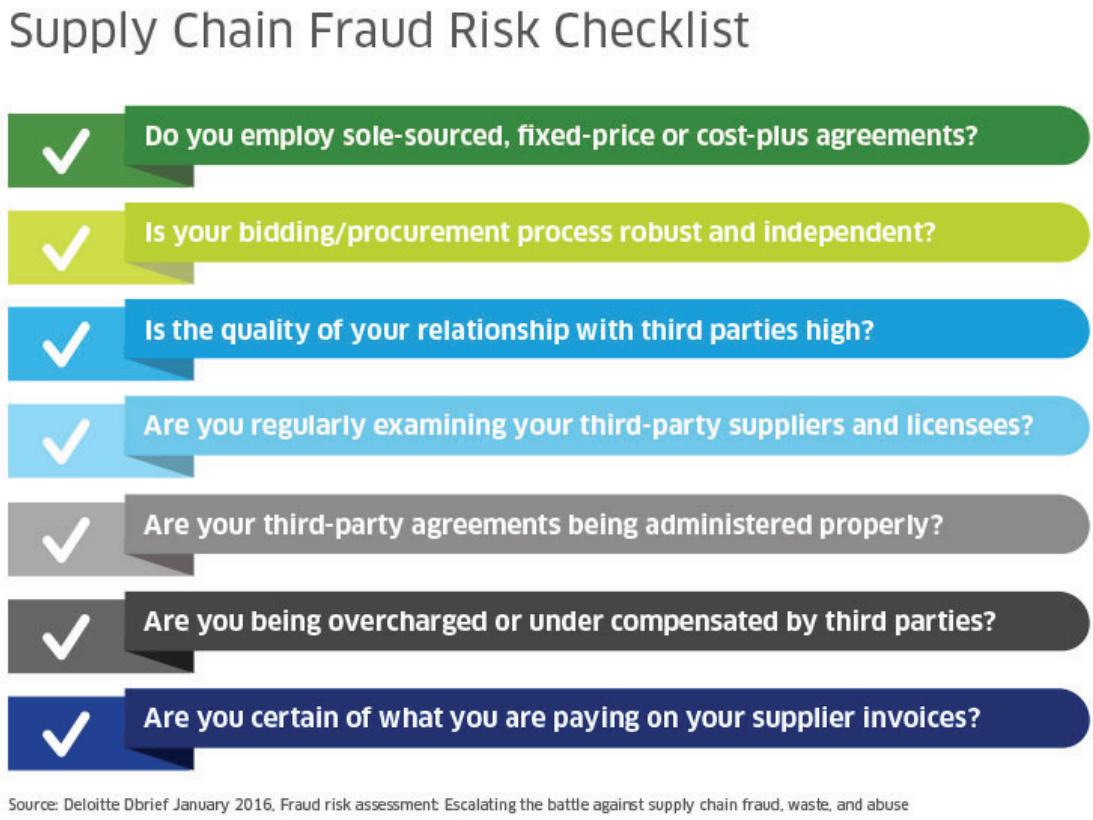
Though compliance resource constraints are often blamed for the lack supply chain fraud prevention and detection programs, Pearson believes that the real reason is more fundamental. “Fraud is a tough topic. It’s like talking to your kids about the birds and the bees, it makes people uncomfortable,” he said.

30 percent of companies experienced supply chain fraud, waste or abuse in the past year, yet 26.8 percent have no program in place to prevent and detect those risks

While most executives don’t want to believe that employees and colleagues may be acting unethically, the Deloitte poll found that employees were identified as the top source of supply chain fraud risk (22.9%), followed by vendors (17.4%) and other third parties (20.1%), including subcontractors and their vendors.

But, with increasing fraud triggers, including volatility in the market, increased globalization and the relative explosion in online-only vendors, it is more critical than ever to have a strong understanding of who you are doing business with, said Pearson. “Organizations should look at supply chain fraud as an element of their broader supply chain risk strategy. Most companies are doing at least some form of non-fraud based risk assessment across their supply chains, they just need to extend that process to include the fraud piece.”

Mark Pearson, Forensics & Investigations, Deloitte



(https://chapters.theiia.org/chicago/Annual%20Seminar%20Presentations/C2%20-%20Supply%20Chain%20Forensics.pdf)

Companies taking a more leading edge approach to mitigating supply chain fraud are using analytics as part of their ongoing invoicing process, said Larry Kivett (http://www2.deloitte.com/us/en/profiles/lkivett.html), partner, Forensics & Investigations practice of Deloitte Financial Advisory Services LLP. "The companies are using data already resident in their ERP systems to run fraud tests and other data analytics which gives them an opportunity, for example, to catch a billing discrepancy before a check is issued. Once the cash is out the door, it is hard to get that money back."

Larry Kivett, Forensics & Investigations, Deloitte

Kivett and Pearson run Deloitte's supply chain forensics service. Using common forensic accounting techniques, they can drill through a client's data to create greater visibility and identify (then mitigate) supply chain fraud, waste, or abuse.

Though analytics may play a critical role in helping companies identify and mitigate supply chain fraud, the effort starts with education. "A big part of what we do is simply making businesses aware of what their risks are. They often get so focused on operational efficiencies, etc. that they aren't necessarily thinking about the financial, brand and reputational risk related to who they are doing business with," said Kivett. "But, if you know where to look, the red flags can help you focus limited resources to drive supply chain transparency and efficiency while reducing fraud, waste and abuse risks."

For Clarke Warren, global compliance director of fraud and forensics at Johnson Controls, one of the biggest challenges is getting people to understand that fraud mitigation is a shared responsibility. "We need somebody in procurement who knows how to identify potential lower cost, reliable suppliers and vendors, and we also need that person to understand that the sales people and project managers from operations have some valuable input on what type of supplier should be used and what's the history of certain suppliers in the field. However, we also need sales and operations to let procurement do their job and understand that we cannot simply use suppliers because they are customer-directed or 'friends' of the company."

Many professionals would rather turn a blind eye to supply chain fraud than to admit its happening within their organization.

Like Pearson, Warren, who was previously senior manager for Ernst & Young LLP's Fraud Investigation and Dispute Services practice (FIDS), sees that many professionals would rather turn a blind eye to supply chain fraud than to admit its happening within their organization. "There is still this 'it can't happen to me' notion."

(https://chapters.theiia.org/chicago/Annual%20Seminar%20Presentations/C2%20-%20Supply%20Chain%20Forensics.pdf)

Keeping tabs of operations without creating a "big brother" atmosphere is another challenge, said Warren. "I have found that one of the best approaches is to implement a continuous monitoring program," he said. "This may sound like 'big brother' to some, but when you set up certain tests using data analytics those tasks can have multiple uses, without significantly impacting the daily lives of others. For example, if I am looking for duplicate invoices, there could be multiple reasons for a potential duplicate highlighted by the analytics. One possibility is there was an unintentional processing of the same invoice twice. Another is an attempt by a vendor to intentionally (or unintentionally) double bill; and still another scenario could involve internal and external parties working together to defraud the company through fake vendor accounts. With continuous monitoring, we can identify those types of outliers and better protect the business without making people feel like you are watching them."

Procurement Fraud Red Flags

- Inconsistent data across procurement-related systems
- Data quality issues relating to spend data and vendor data
- Lack of transparency of procurement data
- Lack of controls around use of preferred vendors, negotiated contracts
- Low compliance with corporate preferred buying guidelines
- Buying power not fully leveraged due to lack of reporting/knowledge of historical spend
- Multiple instances of the same vendor within master file
- Inconsistent vendor payment terms across the organization
- Lack of controls around vendor creation and management
- Failure to actively manage high-risk vendor relationships
- Duplicate payments
- Inefficient invoice processing
- Failure to optimize cash flow and payment terms to vendors and suppliers
- Limited segregation of duties involving payments, credits, and reconciliation of vendors

Source: PriceWaterhouseCoopers, "The Facts About Risks in the Procurement Cycle

Regardless of the kinds of analysis an organization may employ, the most fundamental part of the effort is understanding who you are doing business with, Warren noted. "The most important part of this is the supply chain and procurement people working with the business requesters – sales or operations – to make sure they have done enough due diligence to add these third parties to the supply chain."

An increasingly important part of that due diligence is understanding the different iterations of conflicts of interest. "Companies need to continually assess due diligence procedures because the way people create relationships to take advantage, both internally and externally, are changing all the time. It might not be a wife or family member; rather it could be a close friend, a former employee, or a current employee using a grandparent's bank account to set up a fake vendor. The ways people are getting around controls to hide conflicts of interest are always changing."

Also in this section:

Executive Commentary: Never Again…Until Next Time (http://avtsupplychain.staging.wpengine.com/article/july-2016/never-again-until-next-time/): Why Many Companies Fail to Learn from Their Mistakes. University of

Texas Professor Francisco Polidoro provides some provocative new insight into the organizational dynamics that cause many companies to repeat the same mistakes over and over again.

Executive Commentary: Is It Fake? (http://avtsupplychain.staging.wpengine.com/article/july-2016/is-it-fake/): Renowned hacker and entrepreneur Andrew "bunnie" Huang gives SCN readers a sneak peek into his soon-to-be-released new book "A Guide to Electronics in Shenzhen," with some insider tips on the challenges of sourcing components in China.

Related Resources:

- Blog: Not Far Enough? DFARS Counterfeit Rule Falls Short (blogging.avnet.com/weblog/avnetvoices/2016/05/02/dfars-rule-falls-short)
- Article: A New, More Treacherous Counterfeit Threat Emerges (http://www.sdcexec.com/article/12099861/a-new-more-treacherous-counterfeit-threat-emerges)
- Standards: SAE International AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition (http://www.sae.org/)
- Tool: Water Footprint Assessment (http://waterfootprint.org/en/resources/interactive-tools/water-footprint-assessment-tool/)
- Video: The War on Water with Johan Röckstrom and Randy Sargent (https://youtu.be/VufFi6a_y5M)
- Water Scarcity Solutions: Catalogue of best practice solutions to addressing the growing water scarcity challenge (https://www.waterscarcitysolutions.org/)
- Report: The facts about risks in the procurement cycle (https://www.pwc.com/us/en/forensic-services/publications/assets/cracking-down.pdf)
  (Ed. Note: though this is a bit dated [2007] there is a lot of good insight still to be had)
- Webcast: Fraud risk assessment: Escalating the battle against supply chain fraud, waste, and abuse (http://www2.deloitte.com/us/en/pages/dbriefs-webcasts/events/january/2016/dbriefs-fraud-risk-assessment-escalating-battle-against-supply-chain-fraud-waste-abuse.html)
- Podcast: Eric Pillmore, former SVP of corporate governance at Tyco, on rebuilding trust after crisis (http://www2.deloitte.com/us/en/pages/risk/articles/resilient-podcast.html)