SUPPLY CHAIN CYBERSECURITY

A Report on the Current Risks and a Proposal for a Path Forward

Tony Scott, CEO of TonyScottGroup

Former U.S. CIO and Current Senior Advisor for Cybersecurity and Privacy

Table of Contents

Introduction

For the last few years,[1] supply chain cybersecurity issues and concerns in the information and communications technology (ICT) industry have been a headline-grabbing phenomena, animating a response from legislators[2], regulators[3], industry consortia[4], non-regulatory agencies[5], and a host of other interested parties on a search for solutions.

While supply chain cybersecurity is a subset of the overall cybersecurity landscape, the failure to adequately address important issues may have a significant negative impact in terms of economic outcomes (international trade, commerce), political outcomes (trust in government), and social outcomes (trust in other institutions).

Indeed, the growing importance of ICT for maintaining national security, public safety and law enforcement, national economic well-being, and the privacy of personal and organizational data means that cybersecurity really matters. It is not just a concern about data breach and identity theft – it is a reality about the risks we face regarding the availability of critical services and the resilience of our critical infrastructure. This dependence and criticality will only increase in the next few years with the growth of 5G and IoT.

[1] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf
[2] https://www.govinfo.gov/content/pkg/BILLS-115s3085is/pdf/BILLS-115s3085is.pdf
[3] https://fcw.com/articles/2018/03/26/usf-fcc-supply-chain-cyber.aspx
[4] www.opengroup.org/forum/trusted-technology-forum
[5] https://www.csoonline.com/article/3322018/security/with-supply-chain-security-grabbing-headlines-nist-moves-to-set-new-guidance.html

A Worrying Trend

As incidents related to theft of intellectual property (IP), trade secrets, product plans, personal information, and even political plans and strategies increasingly make headlines, public trust in technology is rapidly eroding. Such recurring incidents have led to a more widespread belief that technology is regularly being weaponized for illegal purposes by criminals, hackers, political activists, private sector institutions and nation states. Knowledgeable leaders in U.S. military, intelligence, private and government entities are championing the clarion call that our national security is at risk as well.

It is projected that this year, more than $100 billion will be spent on various defensive cybersecurity technologies worldwide such as anti-virus, firewall, intrusion detection and prevention, and other endpoint and network protection technologies[6]. It is highly probable a fraction of that amount is spent on supply chain cybersecurity issues, even though the potential for harm is exponentially higher in the U.S. due to the vulnerability of the nation's communications networks and other critical infrastructure. The explosive growth of devices connected to the internet and the greater use of highly scalable cloud and network ecosystems also serve as catalysts to these growing concerns. As an example: in December 2018, a simple licensing issue with a third party supplier brought down O2, the largest mobile provider in the UK, leaving millions across Europe and Asia without wireless services[7]. While this was not caused by any malicious intents, the impact was clearly devastating for the affected operators.

One can imagine the potential global impact of an intentional supply chain compromise of popular consumer devices like phones, home security devices, and automobiles, or in the ever-growing cloud infrastructures that support these devices.

Furthermore, executives in charge of public/private enterprises and institutions have become increasingly concerned about supply chain cybersecurity risks that might expose sensitive/confidential organizational information like customer data, product plans, or financial information[8]. Regulations like the EU's GDPR[9], and California's CCPA[10] add additional incentives for organizations to be concerned about exposure of any personal data that the organization has collected. The penalties are serious. GDPR fines can be as much as €20 million, or four percent of global revenue, whichever is greater.

Most recently, it was reported that computer hardware vendor ASUS[11] was the victim of an attack on the ASUS Live Update tool which deployed malware to thousands of ASUS laptop owners – an example of the weaponization of tools that original equipment manufacturers (OEMs) use in their digital supply chain. Nearly all OEMs use some form of tool like ASUS's, and, if compromised, it could have devastating effects on consumers, businesses, and governments.

Most importantly, an attack by a nation state actor has the potential to disrupt and threaten major portions of the American economy, military defense capabilities, and critical infrastructures, as so many have warned[12].

[6] https://www.idc.com/getdoc.jsp?containerId=prUS44935119
[7] https://www.zdnet.com/article/o2-network-outage-ends-heres-what-happened.
[8] https://businessinsights.bitdefender.com/ceos-highly-concerned-cyber-security.
[9] https://eugdpr.org.
[10] https://www.oag.ca.gov/privacy/ccpa
[11] https://www.eweek.com/security/asus-confirms-attack-against-update-tool-that-exposed-users-to-risk
[12] https://www.csoonline.com/article/3024873/how-much-at-risk-is-the-uss-critical-infrastructure.html

How Did We Get Here? An Implied Trust Model Is Broken

Historically, information technology (IT) providers "owned" a significant portion of the "stack" – the hardware and software components that made up a given solution. The old saying that "Nobody ever got fired for choosing IBM" was partly based on the built-up trust that IBM had accrued over time and the assumption that IBM would be the single accountable party for any issues in the hardware, software and services it provided. Generally speaking, IT buyers could rely on a supplier to have done the necessary integration and testing of hardware and software components, and similar to the IBM model, that same supplier was responsible for the maintenance and monitoring of what it had sold. In such historical arrangements, the OEM suppliers had a high degree of control over their supply chains, and in turn a high degree of implied trust that their supply chain was reliable.

As ICT networks and systems have converged, and will continue to do so with the availability of 5G and IoT technologies, the number of IT and communications component suppliers have expanded internationally, with some concentrating in non-U.S. locations such as Korea, Japan, Taiwan, and China. With the market growing more and more competitive over time, the old IBM model has slowly given way to a landscape where components are globally sourced from a narrower set of dominant suppliers that are low-cost producers. In particular, China has emerged as a major source for many of the minor components that are used in ICT technologies, no matter where the original design originated or where the final assembly of the finished product takes place.

At the very end of this globally diversified supply chain is the customer, who, in many cases, has no idea where all the parts and components originated, or where they may have traveled from, in the journey to becoming a finished product. In any given environment, it is now the de facto reality to see solutions (hardware, software, etc.) from a multitude of vendors. Even when working with global OEMs, there is a strong likelihood that significant portions of their technological products have been sourced (in whole or in part) from non-U.S. sources. In this modern model, key questions have emerged, such as: *Who is responsible for assuring that each of the components individually and collectively meet the quality, security and performance requirements of the buyer? Who is responsible for the end-to-end integrity of the solution? What are the tests and protocols put in place for knowing which components are worthy of trust?*

Quite often the assumption is that the last entity in the supply chain becomes contractually responsible because almost no end-customer (1) wants this responsibility, or (2) possesses the skills internally to assess and manage the risk effectively, and correct any deficiencies that might exist.

To mitigate this accountability burden, suppliers at all levels of the supply chain are increasingly being asked to provide greater visibility and traceability to the origin of the components they use in developing their parts. Often, this takes the form of unique, one-off contractual requirements, including attestation claims, chain of custody, and additional liability requirements for supply chain issues.

The 2018 revision to the NIST Cybersecurity Framework (CSF), and the 2017 Executive Order (EO) mandating that federal agencies use the Framework, reinforce the notion that a risk-based approach is the most practical and cost-effective way for federal agencies to deal with this problem.

With hundreds of ICT enterprises, and millions of customers and end users, it is obviously impractical in the long run to have customers be the focal point for supply chain cybersecurity risk assessment and mitigation. Yet, that is essentially what happens today – an organization's IT department and procurement team come up with contractual requirements and obligations for supply chain risk management, and, specifically, the Chief Information Security Officer is often held responsible for testing, validation, and security integration of a nearly infinite number of combinations of hardware, software, and services. Some alternative approaches are suggested later in this report.

New and Malicious Actors Enter the Scene

Exploiting the ever-expanding surface area of the technology industry and the lucrative nature of many parts of the technology ecosystem, some new “actors” have arrived on the supply chain scene in the form of suppliers of fake and counterfeit parts, suppliers of mislabeled and scavenged parts, and suppliers whose components or products has been deliberately altered (knowingly or unknowingly) to perform a malicious function. With every legitimate supplier selling authorized parts, it is likely that there is a parallel cottage industry that has the ability and capacity to produce fake parts, or in some cases actually use the original production facility and/or expertise to produce compromised parts.

In some cases, it is not an entire organization that is to blame for an intentional compromise of the information systems – it can be as simple as one person or a handful of “insiders” in the organization who are motivated to alter the design or implant malware in the products, networks, or systems that are not equipped to handle these attacks.

This can happen, in fact, at any point or multiple points in the supply chain from design, manufacturing, and packaging to shipping to after sales service/support.

No matter the source, such breaches can have severe national security and economic consequences if not discovered and mitigated effectively. In addition to well-known examples like the Target breach (economic), or the hacking of the U.S. Government Office of Personnel Management (national security), potential targets could include critical infrastructure such as nuclear power plants, health and safety (Center for Disease Control, hospitals, pharma companies), and industrial output institutions (manufacturing, food processing, etc.).

Companies Damaged by Supply Chain Cybersecurity Issues

Most large OEMs and major technology providers now understand that even the accusation of a problem in their supply chain can cause significant financial and reputational damage. Following a recent Bloomberg article about supply chain cybersecurity issues between Apple, Supermicro, and Amazon, the corporations all responded forcefully to the article’s assertions that compromised Supermicro servers were sold to Apple and Amazon. Even though the companies insisted that multiple, thorough investigations corroborated that no such problem ever existed[13], this speculation alone was enough to cause Supermicro’s stock price to drop by 41 percent following the report and it has not significantly recovered since[14]. Whether or not the Bloomberg story was accurate, this still goes to show that supply chain cybersecurity risks are REAL and need to be addressed strategically in a timely manner. Experts say that sophisticated cyberattacks like those in the Bloomberg story are possible.

[13] https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond
[14] https://www.marketwatch.com/story/new-cloud-over-super-micro-adds-to-its-dark-relationship-with-wall-street-2018-10-04

Current Best Practices

As in many other cybersecurity-related areas, currently the most effective approach to managing supply chain cybersecurity risk is to use one of the risk-based frameworks (e.g., NIST CSF), to participate in industry consortia that help develop standards (e.g., Open Group Trusted Technology Forum, ISO/IEC 20243), and to work with regulatory and governmental bodies such as the FCC and DHS, as well as others.

These efforts have had a positive effect on raising awareness and providing some positive proactive steps that organizations can use to address these important supply chain issues. Nearly all agree that a risk-based approach is the most effective way of dealing with these issues, as an analysis of the likelihood of occurrence, and the severity of the impact, can help direct precious resources into areas where they can be most effective.

Relevant publications and standards that can serve as a useful guide:

NIST SP 800-161 (April 2015)**; see also, OMB Circular A-130**

DFARS 252.246-7007 *(48 CFR 252.246-7007)* Detection and Avoidance of Counterfeit Electronic Parts (August 2016)

DFARS 252.246-7008 *(48 CFR 252.246-7008)* Sources of Electronic Parts (May 2018)

ISO 20243 / Open Group Trusted Technology Provider Standard *(O-TTPS)* (2015)

ISO 27036 Information technology -- Security techniques -- Information security for supplier relationships (2016)

NIST-IR 7622 National Supply Chain Risk Management Practices for Federal Information Systems (October 2012)

National Defense Industrial Association *(NDIA)* Guidebook, Engineering for System Assurance (2008)

Supply Chain Risk Management: A Compilation of Best Practices: Supply Chain Risk Leadership Council *(SCRLC)* (Aug 2011)

Customs-Trade Partnership Against Terrorism *(C-TPAT)* Supply Chain Risk Assessment (Mar 2012)

SAFECode Fundamental Practices for Secure Software Development (March 2018)

NIST SP 800-53 R4 (Jan 2015)

SAE AS5553B Counterfeit Electrical, Electronic, and Electromechanical *(EEE)*

Parts; Avoidance, Detection, Mitigation, and Disposition (Sep 2016)

Some companies have taken comprehensive steps throughout their supply chain to minimize the risk of external intervention, including practices such as:

Regular background checks for critical roles in supply chain management	Multiple suppliers for critical components or for essential services
Limiting visibility to customer identity through supply chain lifecycle	Traceability of parts and components from point of origin
Pre-ship and post-ship validation and testing against specifications	Third-party components and software security checks
Segregation of duties verified by audits and controls	Management and governance of source code through the full software lifecycle including management of the ongoing software bill of materials (SBOM)
Active governance of supplier management team by dedicated cybersecurity unit	Product validation and replication testing
Supplier Audits for compliance to specifications	

Government and Regulatory Response

Despite some recent efforts[15], there has been little progress by governments in developing – much less implementing – a comprehensive approach to assess/address cybersecurity-related supply chain risks. The reality is that sophisticated, resourceful, and determined malicious cyber threat actors – including a number of nation states – have the ability to implant exploitable vulnerabilities and hidden functionalities at any point along the global ICT supply chain. These vulnerable networks, systems of owners, and operators can be affected at any time and in a manner of the attacker's choosing. And these implants can be very difficult to find without a serious, focused effort.

Regardless of whatever else might be done to mitigate risk, this reality requires the development of a comprehensive approach to cybersecurity supply chain risk for all ICT vendors and suppliers. Anything short of that represents either a lack of understanding of the real threats in cyberspace or a lack of serious commitment to address it.

[15] https://www.dhs.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology

What Is Unlikely to Work

Some legislative and regulatory proposals take the simple approach of “banning” the use of certain named products or technology from certain suppliers. In some more extreme cases, these proposals ban a named supplier altogether, more common when the supplier is a mainland China-based enterprise. This is usually because of the misconception that some nation states (China in particular) can have undue influence over native companies’ supply chain and product integrity, and as such, can force the company to share sensitive information with the government. Another misbelief is such nation states have the power to authorize ICT suppliers to implant exploitable vulnerabilities and even hidden functionalities. From there, the thinking goes, these establishments are able to conduct illegal surveillance, collect sensitive data, and even launch cyberattacks that can disrupt networks and cause harmful kinetic consequences.

This line of thinking that supports banning such states, companies or technologies is flawed for several reasons. First, it creates a false sense of security that eliminating these products or suppliers renders the supply chain significantly more secure when, in reality, this opens the door for sneaking vulnerabilities and malware much easily and more cost effectively. Second, such an approach to ban products or entire suppliers is not only unlikely to be effective in addressing the critical underlying issues, but also such proposals (if implemented) can come at a significant cost. Customers have fewer choices when competition is limited, and, on a macro level, such decisions can have unintended consequences related to trade (tit for tat retaliation)[16]. It’s important to note that global technology standards are strongest when all players come to the table (as opposed to nation-state isolation) so that the value of intellectual property in the global marketplace is more likely to be respected and preserved. Examples are ISO-27011/ITU-T X.1051, code of practice for information security controls for telecommunications organizations, and the 3rd Generation Partnership Project (3GPP) for mobile telephony – in effect creating a “mobile broadband” standard[17].

It is well understood within the ICT industry that a significant portion of underlying components that go into a finished product are sourced from suppliers in China. For example, companies like Apple and Cisco have abundant sources of supply in China. A ban on Chinese components would cripple many U.S.-based and Western Europe-based companies that do not have viable alternative suppliers. Also at risk is the growing Chinese demand for American goods. The market has seen examples in the current trade battle, where Chinese markets have dried up for American farmers, and other exporters of goods made in the U.S.

[16] https://www.marketwatch.com/story/trade-war-watch-these-are-the-us-companies-with-the-most-at-stake-in-china-2018-03-29

[17] The 3rd Generation Partnership Project is a standards organization that develops protocols for mobile telephony. 3GPP is consortium with seven regional telecommunication associations as primary members and a variety of other organizations as associate members. The 3GPP organizes its work into three different streams: Radio Access Networks, Services and Systems Aspects, and Core Network and Terminals. https://www.3gpp.org/about-3gpp/about-3gpp.

A Rapidly Expanding Issue

The concern about cybersecurity risk is likely to grow as technologically advanced countries like the U.S. see digitization of their governments and growth in vertical Industries associated with 5G, IoT, and industrial IoT (IIoT) – ubiquitous sensors, machine-to-machine communications, and automated everything – all of which will likely bring great benefits to society but will also bring significant dependency and risk.

The number of internet-connected devices will mushroom in the next few years, driven by 5G wireless deployment; consumer IoT or so-called “smart” consumer and business devices like speakers, cameras, home appliances, cars, and other connected devices will also proliferate.

In parallel, we can expect a proliferation of IIoT devices that will be present in all aspects of our economy, including healthcare, manufacturing, transportation, agriculture, energy production, and financial services. The likelihood that some form of artificial intelligence and/or machine learning will be deeply imbedded in each of these devices is very high, as is the likelihood that these devices will connect back to large cloud-based services that will provide additional capabilities to businesses and consumers alike. Along with the many benefits that these new technologies will deliver, there will be additional opportunities for bad actors to insert malicious code and compromised components into the ecosystem.

First Steps

One of the first steps in designing any solution is to clearly define the problem that is to be addressed. In this case, the problem can be defined as, “designing and implementing a cost-effective, risk-based, efficient, globally scalable, and vendor-neutral process for assuring the integrity of the supply chain for ICT components and products throughout the lifecycle (i.e., design, sourcing, manufacture, fulfillment, distribution, sustained deployment, and disposal).” In other words, we need to move toward an objective and transparent basis for knowing which products and components are worthy of trust.

For any risk-based approach, it is also important to identify the threats that serve as the starting point for evaluating the risk and proposing risk-mitigation remedies. It is obviously not cost-effective nor efficient to design solutions for little or unknown threats. Further, a risk-based approach helps ensure that resources are allocated appropriately based on the nature of the threat, existence of exploitable vulnerabilities, likelihood of occurrence, and impact of the risk if it occurs.

Cybersecurity Risk Factors for Supply Chain Threats

Types of Threats – Actors and TTPs

The actors associated with malicious cybersecurity activities (and their respective objectives) fall into several broad categories, each with its own techniques, tactics, and procedures (TTPs) that are common to specific activities.

Here's a look at common actors and their goals:

ACTOR	GOAL
Cyber criminals	Financial gain
Hacktivists	Reputation impact, operation disruption
State-sponsored entities	Access to strategic information and IP, human asset compromise, destruction/disruption of government and critical infrastructure, and key assets/functions of society
Insiders	Various
Industrial espionage	Steal trade secrets and IP
Techno-vandals/hackers	Further/bolster individual or organizational reputation

In the supply chain cybersecurity space, considerable concern lies with state-sponsored actors, and then, each of the other types of actors to a lesser degree. That being said, each of them represent a threat, with the magnitude of risk determined by the vulnerability/likelihood of occurrence and the value of the target to the malicious actor.

A special form of threat actor is known as an Advanced Persistent Threat (APT). An APT is capable of a prolonged, targeted cyberattack. The actor usually seeks to gain access to a network, and, once inside, can remain for a long period time. Historically, the goal of an APT attack is to monitor network activity and steal data rather than to cause damage to the network or organization; it is one of the type of threats usually associated with nation states or sophisticated cyber criminals. That said, it is becoming increasing obvious that some APT actors – including nation states – may choose to cause destructive and harmful outcomes to try to achieve political and strategic goals. It has also become widely recognized that many of the tools which these APT actors use have become easily accessible even to less sophisticated actors, are often inexpensive to deploy, can quickly scale to whatever magnitude desired, and can be hidden from detection for long periods of time – months, even years[18].

[18] https://www.nextgov.com/cybersecurity/2018/05/one-cybersecurity-metric-dwell/147895.

Common Types and Forms of Exploits

The most common form of exploitation used by these actors collectively is through leveraging a known vulnerability in the design or implementation of the technology stack. Sophisticated actors will frequently use the least sophisticated method necessary to accomplish intended goals, so as to avoid garnering any attention to themselves. Exploiting a known vulnerability only requires access to a system with a known unpatched vulnerability, and the information that it has not yet been mitigated. For many of these known vulnerabilities, there are patches, work-arounds, or processes that can be deployed to minimize risk. Historically, the vast majority of actual cybersecurity incidents have been due to the failure of the victim organization(s) or institution(s) to deploy known fixes or to put in place mitigation procedures for known vulnerabilities.

Next in frequency of occurrence are known vulnerabilities for which no fix has been identified, or for which the impact of a potential exploit has been determined to be low and therefore not worth the cost and effort to develop and deploy. Again, as is the case with vulnerabilities with a known patch/fix, no excessive effort (other than access) by a bad actor is usually required to exploit the vulnerability.

The least frequently used exploit is known as the zero-day exploit, where a previously unknown vulnerability is discovered and then leveraged by a malicious actor. While relatively rare, the impact can be significant when they do occur – particularly for widely used components within the technology landscape. It's worth noting that a number of governments buy zero-day exploits from the private market to allow them to conduct surveillance or other surreptitious activity against a target.

Malicious Code/Altered Hardware

Once a bad actor has gained access to a system and/or to the infrastructure that supports it, there is opportunity to move around laterally in the environment to install malicious software or hidden functionality and potentially exfiltrate data, or engage in malicious activity such as altering files, encrypting data and system files (a typical ransomware move), or other more serious activity. Sophisticated actors with access to an assembly or manufacturing facility, or to the product or services supply chain, can sometimes implant codes that enable hidden functionalities to be accessed at a future date when triggered by communication from an external source. If the goal is to imbed hidden functionality to be used in a malicious manner in hardware or software on top of a known good base, the actor may have to breach multiple systems so that the modified hardware or software can pass internal quality checks, and will avoid detection by other means.

This is not just a future issue but is true today due to insufficient hardening of networks and protecting those networks against internal threats. Until recently, the focus of many companies' cyber programs centered on perimeter networks protections with little emphasis on "trusted" internal parties and suppliers; fortunately many organizations are getting more sophisticated and are assuming that malicious actors will penetrate their perimeter; accordingly, they are monitoring perimeters and interior traffic, as well as using tools to look for anomalous activity of any kind. Additionally, more are securing and backing up the most critical data, encrypting data at rest and in transit, and segmenting their networks so that the damage can be contained.

Addressing the Full IT System Lifecycle

One must consider the full IT systems lifecycle leading up to the deployed solution to fully address the total surface area of risk. At each step in the lifecycle, there are multiple parties involved and as such, multiple opportunities for the breach of the information systems that support these processes, as well as for compromising the design or operation of the underlying product.

A risk-based solution will prioritize these steps based on the likelihood of compromise during that phase of the lifecycle and the severity of the impact if the compromise were to succeed.

LIFECYCLE JOURNEY

A typical lifecycle journey for an information system installation, from start to end of life**

1. **Design**
2. **Supplier Selection & Procurement**
3. **Parts Fabrication & Parts QA**
4. **Component Assembly & Testing**
5. **System Integration & Software Installation**
6. **Packaging**
7. **Inventory**
8. **Distribution**
9. **Ship to Customer**
10. **Customer Installation**
11. **Customer Operation & Maintenance (includes service & patching)**
12. **Supplier-side Service and Support**
13. **Equipment De-install and Disposal**

LIFECYCLE PARTIES

A partial list of parties involved in the management and operation of the information systems throughout the lifecycle beyond suppliers of components and software*

Original Design Manufacturer (ODM)

Original Component Manufacturer (OCM)

Original Equipment Manufacturer (OEM)

Systems Integrators (SI)

Service Providers (SP)

Managed Service Providers (MSSP)

Open Software Solutions (OSS)

Transportation and Logistics Companies

Facilities Providers (data center, etc.)

Service and Repair

Asset Recovery & Disposal Companies (ITAR, ITAD)

Customer (IT, procurement, facilities, security, finance, etc.)

Network Providers (e.g., ATT, Verizon, BT, etc.)

**The number of parties involved in a particular lifecycle activity can increase cyber risk because of hand-offs, the number of people involved, and because of more nuanced responsibility for outcomes.*

***Logistics and handling (and physical security for facilities) are not included for steps 3 through 8 as these practices will vary because some OEMs are more vertically integrated and rely less on third parties for some of these steps, and some are much more outsourced and simply act as a final assembler (if that) for their finished goods.*

“Opportunity Time” as a Risk Factor

One must consider the full IT systems lifecycle leading up to the deployed solution to fully address the total surface area of risk. At each step in the lifecycle, there are multiple parties involved and as such, multiple opportunities for the breach of the information systems that support these processes, as well as for compromising the design or operation of the underlying product. A risk-based solution will prioritize these steps based on the likelihood of compromise during that phase of the lifecycle and the severity of the impact if the compromise were to succeed.

“Level of Difficulty” as a Risk Factor

Another often-overlooked factor in analyzing supply chain cybersecurity risk is the level of difficulty to carry out a potential compromise. It may be obvious, but nearly all malicious actors (including nation states) tend to favor low-barrier attacks. These are easier and cheaper to execute versus a more complex exploit, which demands more expertise and resources. It’s also true that the more complex the attack, the easier it is to detect and attribute to a more sophisticated attacker.

A Potential “Risk Scorecard” Approach

Applying the above criteria, a matrix can summarize these various factors and provide an overall “score” to align on cybersecurity priorities.

This can also be thought of as a rating that could predict the likelihood of success.

A sample (not the results of an actual analysis) matrix:

PHASE	TIME*	LEVEL OF DIFFICULTY**	NUMBER OF PARTIES***	SCORE
Design	3	1	1	**5**
Supplier Selection & Procurement	3	1	1	**5**
Parts Fabrication & Parts QA	2	3	1	**6**
Component Assembly & Testing	2	2	3	**7**
System Integration & Software Installation	1	3	3	**7**
Packaging	2	3	1	**6**
Inventory	4	3	1	**8**
Distribution	2	3	1	**6**
Ship to Customer	2	3	1	**6**
Customer Installation	3	4	3	**10**
Customer Operation & Maintenance (includes service and patching)	5	4	3	**12**
Equipment De-install and Disposal	3	3	2	**8**

*TIME	1-5 (1=hours, 2=days, 3=weeks, 4=months, 5=years)
**LEVEL OF DIFFICULTY	1-5 (1=extremely, 2=very, 3=moderately, 4=somewhat, 5=lowest level)
***NUMBER OF PARTIES	1-3 (1=few, 2=several, 3=many)

In the example above, it is clear that the customer installation and customer operation phases in the lifecycle are the ones that present the greatest risk, and thus, are potentially the areas where the most significant investment in prevention, detection, remediation, and recovery are most warranted.

Targeted or Broad Deployment Goal

Another factor to consider in designing a risk-based supply chain cybersecurity solution is whether the threat actor is likely targeting a narrowly defined objective (e.g., a specific person or a specific function within an institution) or is aiming for a widespread set of objectives (e.g., a number of organizations or a particular industry).

A targeted attack usually requires in-depth knowledge of the environment, which in turn requires time and resources in order to map out and plan the attack. A defense against this type of an attack might require a different strategy and set of resources than a defense designed to ward off a very broad set of attacks launched on the organization(s). Similarly, a targeted attack through one of the potential insertion points in the supply chain will also mean a different cost and resource commitment by the bad actor.

A Growing Crisis and Learning from History

Despite the work that has already begun in the supply chain cybersecurity space, it is apparent that the efforts to date have been fragmented. This fragmentation has hampered performance, implementation, and the industry's ability to reach a broad consensus on how best to address risks associated with supply chain cybersecurity. And, as mentioned above, it is likely that with the forthcoming impact of 5G cellular technology, the digitization of vertical industry sectors[19], national dependence on technology, and its attendant risks will inevitably grow.

There are prior moments of crisis in history and lessons learned from such watershed moments can inform the path forward.

One such example is the "quality" crisis that the U.S. faced during the '80s and '90s. At the time, manufacturing in the U.S. was severely lagging behind Japan, Germany, and other countries in terms of the quality of products. This was particularly visible in the automotive industry, but it affected other manufacturing organizations as well, including appliances, machine tools, and industrial equipment.

In 1987, the U.S. Department of Commerce launched the Malcolm Baldrige National Quality Award in response to the quality crisis[20]. Every year thereafter, the award recognized the top quality performers within the auto industry. For many years, this set of awards was presented by the U.S. President and were considered a highly coveted recognition. Every year, hundreds of organizations submitted award applications and the review committee established a positive reputation for being consistent, thorough, and fair in their evaluation and standards.

The agreed importance of this award had a very healthy "trickle down" impact on suppliers and on the whole manufacturing ecosystem. In short order, U.S. manufacturing significantly improved in both quality and overall competitiveness that in turn boosted the economy for many years. Its success can be seen in the fact that most successful manufacturing organizations now have deeply imbedded quality programs and processes in their organizations. Rather than it being a "special" program, "quality" is now just a standard, required feature of their business processes. This too must be incorporated in supply chain management by the players in today's ICT ecosystem.

Another example of the industry coming together to address a common issue is the PCI[21] standards that have been widely adopted for credit card processing. The PCI security standards and related processes were created in response to widespread fraud in the credit card industry. While heavily focused on institutions that accept credit cards and process them, an entire ecosystem has emerged around the PCI standards to the degree that they are now the norm in the payment card industry.

A final example of a case where government and institutions have come together to address a widespread issue is an industry is the Bank Secrecy Act[22] (BSA), developed to address money laundering. Anti-money laundering technology (primarily software) is an effective means of detecting and reporting fraud/theft, and there is widespread acceptance of this technology across financial institutions.

[19] For example, the enhanced use of sensors, machine-to-machine communications driving industrial control systems and machine/robot responses, such as: autonomous driving, remote surgery, eManufacturing, green energy and smart agriculture and smart cities, and continued proliferation of consumer IoT devices.

[20] https://baldrigefoundation.org/who-we-are/history.html.

[21] https://www.pcisecuritystandards.org.

[22] https://www.occ.treas.gov/topics/compliance-bsa/bsa/index-bsa.html.

Missing Players from the Current Discussion

In much of the discussion to date, the focus has necessarily been on ICT component suppliers, including hardware and software vendors, and the needs of their customers to understand and address their supply chain risk. Customers' needs include assurance that the components they buy cannot easily be exploited to perform tasks contrary to their interests. The risks are high from the customers' perspectives, including the possible exfiltration of their critical data, the destruction/alteration of important information, and even the ability to launch cyberattacks to disrupt or cause significant physical consequences (like Stuxnet).

However, a key factor often missing in the discussion of ICT supply chain risk is the role of the carriers and internet service providers (ISPs) such as AT&T, BT, Verizon, etc., and their responsibilities (or lack thereof) with regard to mitigating cybersecurity risks in operations, especially with their suppliers[23]. Because these entities are responsible for managing the network highways that transfer data, including the fruits of malware and cybersecurity exploits, it stands to reason that these carriers must be a part of the ultimate solution that appropriately manages risk. Just like the driver of the "getaway" car in a bank robbery, carriers and ISPs that allow or facilitate the transmission of stolen data or allow their networks to be infiltrated by nation states, cybercriminals, hackers, and the like, must be held responsible and accountable for these actions. Accordingly, they must play a much bigger role in addressing real supply chain cybersecurity risks, including the prevention, detection, and at least partial mitigation of the potential impact of this kind of breach.

The recommendations of FCC's advisory group, Communications Security, Reliability and Interoperability Council[24] (CSRIC), are a useful starting point, as are their recommendations to address risk from the upcoming deployments of 5G network technology. The recommendations – together with those of the National Security Telecommunications Advisory Committee (NSTAC) – can help avoid a cyber crisis in the future that could be exponentially worse than anything we have seen before because of vastly increased network bandwidth, the virtualization of network functions, and changes in network architecture.

[23] See, for example, ISO 27011.

[24] https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-1.

The Costs of Inefficient Buying and Procurement Activity in Supply Chain Risk Management

One factor that is sure to resonate with IT buyers and sellers is the cost associated with non-standardized contractual clauses related to supply chain cybersecurity assurance. Today, nearly every buyer in the ICT industry includes varying requirements related to supply chain risk in its contract clauses and provisions. These can be liability clauses, inspection rights, transparency and reporting requirements, and other remedial activities, often exacting high costs that are ultimately baked into the cost of the products. The more non-standard these contractual requirements are, the higher the total cost.

Purchasing power can have a remarkable influence on incentivizing behavior change by ICT vendors so that they raise security and assurance levels for products and services. It is very important for organizations to use their risk-informed purchasing power – appropriate to the business objectives and risk environment – and to collaborate with like-minded buyers. Leveraging their purchasing power to incentivize ICT (and other IT) vendors to raise the assurance characteristics of their products and services is key.

Such recommended requirements, used successfully over time, can be referenced and incorporated by regulatory bodies into mandatory requirements for the highest risk environments, such as for government and critical infrastructure. Examples of such efforts include the EastWest Institute Buyers Guide for ICT[25] and the SAFECode Fundamental Practices for Secure Software Development (Third Edition)[26].

[25] https://www.eastwest.ngo/idea/eastwest-institute-launches-cybersecurity-guide-technology-buyers.

[26] https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf.

The Need for Independent Third-Party Testing

One current issue in the technology industry is the absence of a globally or regionally recognized authority or service – or even an assurance framework – for testing components (hardware, software, etc.) for cybersecurity risk; for encouraging buyers to develop and use recommended procurement requirements; and for encouraging ICT vendors to develop their own, agreed-upon best practices for assurance and transparency.

If an organization wants to have a device tested or certified, there are companies that will do testing, however, there is no agreed standard or set of best practices to inform this testing or facilitate comparison of the results beyond the visibility of the company and the tester they retained. Suppliers are increasingly being asked to detail and warrant their supply chain practices (see above), but this only mitigates part of the risk. OEMs are naturally reluctant to share engineering design details with customers for fear of loss of IP, and yet validation against the specifications and conformance to a detailed bill of materials are essential to any form of quality assurance validation, which in turn is key to transparency and builds trust.

An independent, non-profit, testing capability – informed by globally agreed requirements and steeped in internationally recognized standards – could be a valued resource to addressing cybersecurity concerns transparently. Design details could be shared in a manner that would not lead to loss of IP, and customers could have confidence that the products they are buying conform to the specifications and requirements that have been promised, the strength of which is informed by input from the global community. To be fully effective, the independent service should be free from political and technical bias, and should be internationally recognized for its objective standards and methods.

The idea of having an approach that facilitates mutual recognition of testing against agreed-upon requirements is not new, and it does not have to preclude the possibility that certain ICT buyers in higher risk environments might conduct their own supplemental product testing. The Common Criteria[27] is such a model, although it is not universally used by any means. The Common Criteria comprises “the Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) [which] are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA).” Pursuant to the Common Criteria:

“[p]roducts can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance; Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies.”

Such a system could be established for cybersecurity product testing. The goal is to test once and trust everywhere, versus the ad hoc nature of today’s testing and certification processes as defined by individual organizations. And, given the reality of the global nature of most supply chains, progress on this could ease concerns that might otherwise impede a healthy, valuable, and vibrant industry across the globe.

The existing security evaluation and accreditation mechanism for the telecoms industry is called the Network Equipment Security Assurance Scheme (NESAS). This is jointly defined and overseen by the 3rd Generation Partnership Project (3GPP) and the GSM Association (GSMA). NESAS is a voluntary scheme defined for the mobile industry to provide a security baseline and comprehensive security audit. It evidences that network equipment satisfies security requirements and that network equipment vendors comply with security standards during their product development and lifecycle processes. The GSMA has an accreditation board, which is responsible for monitoring and developing plans and granting accreditation.

[27] https://www.commoncriteriaportal.org/.

Supply Chain Cybersecurity – One Form of a "Quality" Issue

Some supply chain cybersecurity issues are manifestations of problems around consistency of quality, which can be effectively managed and mitigated by using recognized standards and best practices that have been developed, tested, and proven over a long period of time.

Critical factors that can apply to the supply chain cybersecurity space are:

Leadership – Implement some form of significant facilitating/convening/organizing to get the necessary ecosystem players together initially. This could be led by an independent non-profit organization like The Center for Internet Security[28] (CIS), which has an outstanding reputation for developing and publishing best practices, benchmarks, and configuration guidelines for a broad set of internet-related technologies.

Information and Analytics – Develop consensus on standardized methods for improving supply chain transparency, assurance, and visibility. Develop standardized data and reporting requirements, as well as standardized analysis tools that can be used to measure performance. This should include all lifecycle parties, including suppliers, buyers, distributors and system integrators.

Strategic Planning – Define elements of a strawman institutional plan (for all of the critical parties involved in supply chain risk) that reflect a desire to develop (and improve existing) quantifiable metrics around supply chain cybersecurity. Identify the appropriate resources needed to achieve the desired outcome.

Human Resource Utilization – Draft templates for using an "all-in" organization-wide approach to enhance supply chain cybersecurity metrics and processes. This must include appropriate training, organizational effectiveness metrics, and governance models necessary to accomplish the desired goals.

Quality Assurance and Internal Testing of Products and Services – Ensure a standardized set of appropriate controls are in place to identify supply chain cybersecurity issues on the fly and provide corrective action[29].

Quality Results – Maintain objective external measures of quality (e.g., Six Sigma).

Customer Satisfaction – Create active measures of customer satisfaction with transparency, visibility, management, governance, speed, quality, etc.

[28] https://www.cisecurity.org/.
[29] https://www.iso.org/standard/76070.html.

Next Steps

For any serious progress to be made on the supply chain cybersecurity issues outlined in this paper, these steps seem to be the most logical:

1. Use the power of one or more influential organizations to convene a series of meetings of interested parties – including suppliers, regulators, carriers, industry groups, security experts, and interested members of the public – to explore and recommend a series of prioritized actions that will positively impact supply chain cybersecurity.
2. When appropriate, engage U.S. and international standards bodies to develop/support standards for managing, measuring, and mitigating supply chain cybersecurity risk.
3. Explore the potential viability and effectiveness of an independent third-party testing capability for ICT hardware and software.

Conclusion

Given the magnitude of potential problems associated with supply chain cybersecurity, and the economic and social impact that is likely to accrue if these issues are not comprehensively addressed, it is imperative that a thorough and scalable approach be developed, and implemented, beginning with a model or framework for global ICT assurance. It is essential that governments be engaged with the private sectors to move down a path toward the development of an effective assurance framework. Hopefully, public-private collaboration can lead to a positive outcome so that unconstructive and overly-restrictive legislation and regulation are not enacted.

Most importantly, the time to act is now. The longer that multiple, fragmented efforts continue to develop, the more likely there will continue to be confusion, costs, and conflicts that will impair important uses of information technology to address critical health, safety, and security issues and to create a basis for knowing which products and services are worthy of trust.

Tony Scott is CEO of the Tony Scott Group, and is a Senior Advisor for Cybersecurity and Privacy at Squire Patton Boggs, a prominent international law firm. Until January 2017, he served in the Obama administration as the 3rd Federal Chief Information Officer (Federal CIO) for the U.S. Government, and was appointed to that role by President Obama in February 2015. The Federal CIO has oversight, budget and management responsibilities for the more than $85 billion that the Federal Government annually spends on IT. In that capacity, he created the government-wide response plan after the OPM cybersecurity hacking incident, including the Cybersecurity Sprint and Implementation Plan (CSIP), which dramatically improved the information systems security posture of the Federal Government. His numerous appearances before Congress, and many other forums - providing CXO level public and private sector insight on matters such as digital workplace transformation, cybersecurity, governance, open data, and workforce diversity have been widely recognized.

Immediately before joining the Obama administration, Tony was the Chief Information Officer at Vmware. Prior roles include the Chief Information Officer at Microsoft Corporation, Chief Information Officer at the Walt Disney Company, and Chief Technology Officer at General Motors Information Systems & Services.

Tony holds a Bachelor of Science Degree from the University of San Francisco in Information Systems Management, and a Juris Doctorate (law) degree from Santa Clara University. He was inducted into CIO magazine's “CIO Hall of Fame” in 2009, and has been a frequent keynote speaker, panelist, and advisor at numerous industry and government events. Tony is also a licensed pilot, and enjoys flying his own plane whenever possible.