Whitepaper

The Supply Chain Threat

WITH secure

Contents

1 Introduction

1 Introduction

In recent years, supply chain attacks have been numerous, successful, and highly impactful, the most recent example of which is the 3CX compromise. The obvious success of past supply chain attacks encourages attackers to attempt to replicate those successes, and the web of complex trust relationships that makes up the current technology ecosystem empowers supply chain attacks, allowing a single compromise to affect thousands of organizations. Proof of this impact can be seen in the fact that multiple governments are now proposing legislation to address the chains of trust and vulnerability that have enabled single cyber security incidents to have such far-reaching impact.

This report will:

- Define what a supply chain attack is,
- Explain why they have become more common and successful over time,
- Summarize the EU, US, and UK legislation specifically drafted to address the risk of supply chain attacks,
- Present example incidents and trends in supply chain attacks,
- Discuss the Zero Trust Model, a defense against such attacks,
- Present conclusions and predictions.

2 Supply chain threat overview

2 Supply chain threat overview

A supply chain attack is when an attacker compromises a particular organization or entity, and then leverages that initial compromise against others who have a trust relationship with the initial victim.

Such an attack is possible when two entities have a trust relationship, most typically when one entity trusts another to provide a service. The modern tech ecosystem of service providers and cloud solutions is a complex web of trust relationships, which increases the ease and effectiveness of supply chain attacks in a number of ways.

Trusting another entity increases the attack surface of your network and increases the complexity of your network boundary, both of which can make your network harder to secure.

Well-resourced defenders, such as those at the largest and most commonly used software and service providers, will likely have very good security practices, but the outcome of an attack depends on the actions of both the defender and the attacker. While these organizations may be very secure, they are also very high-value targets – so they are very likely to be targeted, and persistent attackers will keep targeting them. The successful compromise of a large service or software provider could give an attacker access to many downstream victims who trust that supplier.

We can group supply chain attacks into three types:

- Upstream – the true intended victim is downstream from the initial, steppingstone victim,
- Opportunistic – an attacker compromises a victim. Post-compromise they look for the most valuable things on the network – and that happens to be the data or accesses of customers,
- Targeted – a victim is targeted and compromised specifically because they are known to be a supplier of many other organizations, and one successful breach of that supplier could act as a huge force multiplier for the attacker.

In essence, supply chain attacks rely on the fact that all defenders must get it right every time, whereas an attacker only has to get it right once.

3 Factors contributing to the rise in supply chain attacks

WITH secure

3 Factors contributing to the rise in supply chain attacks

In recent years, there have been several wildly successful supply chain attacks. Both the SolarWinds (2020.12) and Kaseya (2021.07) incidents made it clear just what can be achieved by a successful supply chain attack, and are likely to have whetted the appetite of ambitious cyber criminals.

The current tech ecosystem relies heavily on trust relationships and service providers, so supply chain attacks simply make a lot of sense. Infrastructure/Platform/Software as a Service (*aaS) providers must be trusted by their customers as they have access to, or even control over, the information, network and business functions of their customers. As such, the compromise of a single *aaS provider can give an attacker in-depth access to multiple organizations.

Beyond the explicit, contractual trust relationships of supplier and customer, there is also the much wider context of software dependencies and libraries. When importing code libraries or whole applications into a product or solution from a public repository, it may not be clear that there is a relationship with a supplier. In such cases, the public repository acts as a distributor between the author and the user. This brings to mind an old saying about object-orientated programming: In order to write object-orientated code, you search the internet for objects that other people have written, then orientate them in your own code until they do what you want.

3.1 Log4Shell: A special case

Announced in December 2021, the true impact of Log4Shell was only felt in 2022, and it became one of the most significant vulnerabilities of the year. It was commonly found in public-facing services, had a very high severity, and was heavily targeted.

Log4j is a library, or bundle, of code that is designed to be used by other programming projects to provide a particular functionality; in this case, logging. Logging is a pretty basic thing that lots of programming projects need to do, and that lots of other libraries will also need to do. As such, Log4j was incorporated into many other pieces of software as a dependency, and that dependency could be many layers deep and not immediately apparent to the users or administrators of the software.

Most organizations did not know if they were using Log4j, as they had not chosen to do so. They had chosen to use software that happened to incorporate Log4j. Each code dependency is in effect a trust relationship, where the author of one piece of code has decided to trust the author of another piece of code, and the end-user then puts their trust in that entire chain of dependencies.

The first patch issued for Log4j was intended to fix the issue – and it did. But the patch unintentionally introduced a new vulnerability that could cause a Denial of Service, requiring yet another follow-up patch.

Cloud providers such as Amazon provided services that used Log4j, and in those cases patching the vulnerability required Amazon to issue a patch for its customers to apply themselves. However, the Amazon-issued patch for Log4j accidentally introduced three new vulnerabilities (separate to the vulnerability introduced in the initial Log4j patch), which required Amazon to issue yet another patch for customers to apply.

4 Incidents

WITH secure

4 Incidents

4.1 Software providers

4.1.1 3CX

3CX is a software-phone and PBX provider with 600,000 business customers around the world, including large multinational corporations.

In March 2023, 3CX customers found that their phone software, and even fresh copies downloaded directly from 3CX, were being detected as exhibiting malicious behavior by their Endpoint Detection and Response (EDR) solutions. 3CX customers began posting on the company's support forums querying this. Initially, 3CX responded by saying that the EDR solutions themselves were faulty, and that there was no issue. One week later Crowdstrike, followed by WithSecure and multiple other Infosec companies, reported that they had analyzed the 3CX binaries and identified they had been trojanized by an attacker.

The compromised binaries were identified as the infection vector for a multistage attack, which downloads and runs a previously unknown info stealer – most likely to allow the attacker to catalog and identify the huge numbers of victims.

While this attack could have been used to launch a huge opportunistic attack in a similar vein to Kaseya, only a small number of hands-on-keyboard interactions by the malicious attacker on specific victims appear to have occurred at the time of writing. The malware was configured to wait for one to four weeks after installation before connecting to C2 infrastructure for the second stage. Combined with rapid heuristic/behavioral detections of the malicious behavior, this pause means the campaign appears to have been detected very early on in its operations. However, the potential impact of this compromise cannot be overstated.

This is a classic software supply chain attack, where a trusted software developer is compromised, the customers' trust of the provider is abused, and the trojanized product is used to enable access to their entire customer base at once, affecting many thousands of devices and users with a single well-placed compromise.

4.2 Service providers

A number of service providers were compromised in 2022; some suffered from bad security practices. Others were found to have had vulnerabilities in the software and services they used to provide their services to others, though in some cases there was no proof that these vulnerabilities had been exploited.

4.2.1 Zellis

Zellis is a UK-based payroll and HR solutions provider. According to its website, it is responsible for the payroll of five million employees every month and is used by 42% of the FTSE100.

In June 2023, it was discovered that the ransomware group Cl0p had performed a zero-day mass-exploitation attack of more than 300 organizations, including Zellis. The attack leveraged a zero-day vulnerability in the MOVEit Transfer managed file-transfer software. Because MOVEit is used to transfer files, the threat actor was able to, at the very least, steal any data stored on the exploited MOVEit servers. In the case of Zellis, this meant data on the payroll and employees of multiple customers, including the BBC, Boots pharmacy, Sky, Harrods, Jaguar Land Rover, Dyson, and Credit Suisse.

This is an interesting case within the subject of supply chain attacks, because while the MOVEit attacks affected a large number of organizations, there is an argument that, to Zellis, and other directly impacted organizations, it was no more a supply chain attack than any other software vulnerability. Yes, the customers of MOVEit trusted them to provide a secure software solution, but there is no indication that MOVEit the organization was compromised. They were simply providing an insecure product to their customers. However, the compromise of Zellis did turn into a supply chain attack, because the customers of Zellis were compromised through their trust of the Zellis organization.

4.2.3 Heroku

Heroku is a Platform as a Service (PaaS) provider. It provides a cloud environment where its customers can execute their code. This is quite a complex space, as Heroku essentially has to operate between the end-user of its customers' services and the customer's own development pipeline. In addition, many of the development processes used by customers of Heroku are hosted in other cloud services, creating a nexus of interacting trusts and services.

When Heroku was compromised, the attacker was able to gain access to the GitHub code repositories of Heroku's customers and download some of the contents. While it is best practice not to leave user accounts, passwords, encryption keys, or any other sensitive information in a code repository, this often does happen and may have happened in this case. Muddying the waters further is the fact that while Heroku's customers use GitHub, its customers also included a subsidiary of GitHub named NPM, and NPM's code repositories were accessed. NPM itself provides a service to allow users to download and manage software dependencies for their own coding projects, extending and complicating the supply chain even further.

4.2.3 LastPass

LastPass is a company that provides a cloud-based password storage service. In August 2022, LastPass was compromised and its customers' encrypted passwords were stolen, along with other customer data, both encrypted and unencrypted, that customers had stored in their LastPass accounts. LastPass initially stated that only source code was taken but later confirmed that encrypted customer passwords were stolen. Most recently, in early 2023, LastPass confirmed that the stolen data included one-half (the half that is unique for each user in an enterprise) of each of the encryption keys of its enterprise customers, known as K2s. Unfortunately, the other half of the encryption key for each enterprise client (K1) is the same for every user in that enterprise and is available to every user in that enterprise. This means that it would only take one localized compromise to be able to decrypt the entire enterprise vault with the stolen K2s. While keys can be rotated, it is not a simple process and the compromise of the K2s was not made public until six months after it occurred.

4.2.4 Amazon Web Service Elastic Kubernetes Service (AWS EKS)

Kubernetes is an open-source cloud orchestration tool that can be used to automate the deployment and management of containerized applications in the cloud. AWS offers a managed Kubernetes service called EKS. To allow EKS to use AWS Identity and Access Management (IAM) roles (a way to control authentication and authorization in AWS), Amazon provides the IAM Authenticator for Kubernetes.

In 2022, a flaw was found in the IAM Authenticator that would have allowed privilege escalation and the use of replay attacks to authenticate. While this vulnerability was patched before it was announced and thus was never assigned a CVE, it was present in the code of this public-facing service since it was launched five years ago. As such, a very large number of AWS customers were vulnerable for that time. While there was no confirmed exploitation of this vulnerability, it does highlight a key risk of supply chain attacks, which is the sheer number of customers that can be affected by a single issue.

4.2.5 Twilio and Okta

Twilio is an SMS API provider, a service often used by other service providers to secure their own services. Twilio employees fell victim to a targeted phishing/smishing campaign, and through those compromised employee accounts an attacker was able to access customer data. On top of that, however, one of the affected downstream victims whose data was accessed via the Twilio breach was Okta, an Identity and Access Management (IDAM) provider that could be an extremely valuable target for an attacker, due its role as a trusted intermediary for a large number of potential targets.

5 Source Code Theft

5 Source Code Theft

Considering persistent, motivated attackers are looking for vulnerabilities to exploit and possibly sell on, it is possible that access to source code may hold more long-term value than compromising valid credentials for immediate but temporary network access. Indeed, the targeting of code repositories and the theft of source code was another recurring trend in 2022.

5.1 Intel

The processors and electronics hardware that Intel designs and manufactures is one of the foundations of the tech sector, so it is significant that the source code for Intel's new Alder Lake chipset BIOS was stolen and posted online. The impact of this theft cannot be known, but in the past researchers have identified vulnerabilities in the functioning of computer hardware that could be exploited to compromise computer systems, and access to BIOS source code could make it easier for malicious actors to identify vulnerabilities.

5.2 LastPass

We mentioned LastPass earlier as a compromised service provider. As well as that theft of customer data, LastPass source code was also stolen; in fact, the data theft seems to have come from the compromise of the personal device of a senior DevOps engineer. That engineer had access to source code and secrets that allowed access to cloud storage buckets containing customer data.

5.3 Dropbox

Dropbox was successfully compromised in a phishing campaign by an unknown actor; as a result, the contents of 130 GitHub code repositories were stolen. Dropbox has stated that technically, what was stolen was not its source code but merely other code that had been modified and was being used, which makes a rather unclear distinction between code you have modified and code you have written.

5.4 Okta

As well as the supply chain compromise Okta suffered via Twilio, in an apparently separate incident, source code was stolen by an attacker from Okta's private GitHub repositories. Okta has stated that no customer or service data was accessed, and that it does not rely on the secrecy of its source code to keep its products secure. That being said, this was one of at least three compromises suffered by Okta during 2022, and the company has not stated how its private code repositories were accessed. As previously stated, Okta is an IDAM provider, and the nature of its business means it is extremely interconnected. Okta's most recent annual report states it has 7,000 integrations to other service providers available.

6 Poison packages

6 Poison packages

The web of dependencies that underpins almost all modern software has come under examination in recent years, particularly after Log4Shell and Heartbleed, two vulnerabilities in software packages relied upon by many other pieces of software. However, as well as the issue of vulnerable software being included as a software dependency in digital products, which is then used by unwitting end-users, the concept of ‘poison packages’ has come to light. Poison packages are intentionally malicious code uploaded to online software repositories for the purpose of compromise.

6.1 Too good to be true

Software packages have been identified in public repositories that claim to be legitimate, helpful libraries, but instead contain malicious code such as info stealers and backdoors. How do the attackers lure people into downloading them? Simply by claiming that these libraries solve common problems quickly and easily.

6.2 Dependency confusion

Dependency confusion describes an attack where an attacker places malicious code in a public package registry with a name that duplicates or conflicts with the name of a package stored in a private repository, inside the target organization. Because the two repositories are separate, they can both contain packages with the same name.

If a package manager at the target organization is configured to query the public repository before the private one, it will import the malicious code, which will then be executed instead of the intended package. This attack requires both luck and some foreknowledge, but it highlights the use of packages as an intentional vector for targeted attacks.

6.3 Typo squatting

Certain words are commonly misspelled or might be shortened or concatenated into the name of a package in different ways. Indeed, words may just be spelled differently by native speakers of different languages. As such attackers can simply ‘typo squat’ popular packages by uploading their malicious code (possibly hidden inside a copy of the legitimate package) under a similar name to the legitimate package.

6.4 Mitigation

Secure software development practice is simply software development best practice, and it seeks to address these issues and many others. Software repository maintainers are aware of these types of attacks and do their best to address them, but there is an issue of scale. The Python Package Index (PyPI) contains 300,000 packages, while Node Package Manager (NPM) contains over 1,300,000. The vast majority of these packages are benign, but policing that many packages of code is a huge undertaking.

7 Phishing

WITH secure

7 Phishing

Phishing is a pervasive and constant presence. A significant number of compromises come from successful phishing attacks, and it is a tactic used by countless threat actors. Phishing has been in use for decades, and there is no sign that it is going to stop being viable any time soon. At most, the medium may change from email to some other digital message or mail exchange service. The reason it is included in this document is because phishing is most effective when it is abusing trust relationships. When a phishing email is sent from a compromised trusted sender, it has a far higher chance of success. Even if a malicious email is simply made to appear as if it comes from a trusted sender, its success becomes more likely. Phishing emails actively try to abuse trust relationships. When an attacker is attempting to monetize a compromised email account, they will almost attempt to compromise the account's contacts because the existing trust means they are more likely to succeed.

8 Legislation

WITH secure

8 Legislation

The impact of recent supply chain attacks is made clear by looking at the response of world governments. The EU, UK, US, and China have all either proposed or implemented legislation in the past two years specifically to address cyber security, with a particular focus on supply chain security.

These pieces of legislation are:

EU:

- Cyber Resilience Act (CRA)
- Digital Operations Resilience Act (DORA)
- Network Information Security Directive 2 (NIS 2)

UK:

- Proposal for Legislation to Improve the UK's Cyber Resilience

US:

- US Executive Order EO14028 – Improving the Nation's Cybersecurity

China:

- Cyber Security Law (2016) Measures for Cyber Security Review (2020)

While the various pieces of legislation are all different, they do have common themes between them, in that they:

- Define Critical National Infrastructure (CNI) and important digital services/products,
- Require the implementation of security best practices,
- Impose higher levels of responsibility and security on CNI,
- Impose those same higher levels of responsibility and security on the supply chain of CNI entities,
- Require risk management, disaster recovery, and incident mitigation planning,
- Require transparency through threat intelligence sharing and deadlines for incident notification,
- Encourage/require diversification of supply chains.

8.1 Impact of legislation

In effect, these various pieces of legislation require industries and entities that are important to the state to be more secure by implementing security best practice, sharing threat intelligence information and, most importantly, they impose these requirements upon the supply chains of these important entities. Because the important organizations are so large and pervasive, imposing these security requirements on their supply chains means that the vast majority of digital product and service providers will have to operate under these new requirements.

The Chinese legislation was enacted in 2016 but refers to definitions and measures that did not exist at the time. Those definitions and measures are being created now, after the law is in effect, so the exact requirements of the law are not yet clear. This law is more focused on geopolitical factors than generic supply chain, however.

9 Zero trust

9 Zero trust

The Zero Trust Model is intended to defend against supply chain, insider threat, and credential theft attacks. As an information security company, implementing and reviewing zero trust architectures is something that WithSecure regularly consults on.

In some ways, the Zero Trust Model is good old-fashioned paranoia, where you trust no one and verify everything, and it focuses on the following principles:

- **Assume breach** – Put in place controls to contain and minimize the effect of any breach, wherever it happens, or whoever it happens to. Improve your visibility to enable breach-detection, encrypt data wherever possible (especially when it goes to a third party), and act based on the assumption that a breach will happen,
- **Least privilege** – An old and reliable paradigm for implementing permissions, this means that you only give a user or process the privileges and permissions necessary to do their intended role and nothing more,
- **Verification** – Nothing is assumed. Any value, identity, process, or service is explicitly verified. If everything is explicitly verified, then nothing is implicitly trusted, hence the Zero Trust Model.

Zero trust is a concept that has been around for a long time, and in the olden days it consisted of micro-segmentation of networks. In the significant supply chain breaches mentioned in this report, however, network segmentation would most likely have had no effect. It doesn't matter how many firewalls you install if your data or identities are held in the cloud of a third party who has just been compromised.

In the complex cloud ecosystem in which organizations now operate, and in which these supply chain attacks occurred, implementation of a Zero Trust Model means recognizing that the primary security boundary is no longer your network edge, it is your identities, access controls, and cloud secrets.

9.1 Software Development Lifecycle (SDLC)

So how does the Zero Trust Model apply to the SDLC? In theory it's very straightforward and can be summed up by the glib turn of phrase: 'shift security left.' We've given a number of examples of source code theft and of risks from the software supply chain. The risks, and the impact of source code theft, can be minimized by making sure you consider security during your development pipeline, and that it is not simply a tick box before production. Of course, you must also trust your software supplier is doing the same, and so on.

9.2 How to make the Zero Trust Model viable

In a more practical sense, implementing zero trust means defense in-depth. Another tenet of 'assume breach' is the ability to detect and respond to a breach quickly and effectively. Understanding atypical and erroneous behavior of third parties – whether that be software packages, or people you might exchange emails with – is vital. For this to work, organizations cannot simply follow frameworks or purchase technology and recognize that inherent trust in third parties is difficult with no oversight and the amount of high-profile supply chain attacks being observed.

10 Conclusions

10 Conclusions

Service and software complexity has increased dramatically in the past few years.

Complexity alone can make it more difficult to secure an environment, but it also means there are more software and service dependencies in a typical environment, and longer, more complex software supply chains.

In an ideal situation, outsourcing a service means that it will be done better than it could be done in-house, and more cheaply. Even if this is the case, competent attackers will focus their efforts wherever they can get the most benefit, repeatedly and persistently targeting high-value victims.

Recent successful supply chain attacks have made it very clear that high-value victims are not only those that are themselves high value, but victims that can provide access to multiple others downstream.

The actions of governments implementing legislation specifically to address the issue of such attacks makes the case for how very severe supply chain attacks are, and clearly shows that concern about them is not limited to the cyber security community.

11 Predictions

WITH secure

11 Predictions

The direction of travel of the technology ecosystem is towards cloud and managed services with increasing complexity. There is no sign of this being reversed in the future, and indeed current global financial pressures mean that businesses will keep looking for short- and long-term cost savings.

This complex ecosystem will favor supply chain attacks, which are made easier and more effective in such an environment.

As legislation to address supply chain risk comes into force, many organizations will be required to implement security best practices and invest further in their security, as well as that of their customers and suppliers. However, while increased awareness and verification of supplier security will help, the digital ecosystem will remain complex and inherently difficult to verify as secure.

Attackers will continue to use tactics that succeed, and the most successful attackers will not only be able to increase their operational tempo but will likely inspire others to attempt to copy their success.

As such, defenders will need to have a clear understanding of what they are defending, and where they are vulnerable, if they are to be successful, and they will need to be able to answer the following questions:

- Where are your assets?
- Who has access?
- Who controls that access?

12 Appendix

12 Appendix

12.1 A high-level summary of the different pieces of legislation

12.1.1 EU Cyber Resilience Act (CRA)

One of the three pieces of EU legislation, this applies quite broadly, with the following key points:

- Imposes cyber security obligations on all products with digital elements that will or could have a data connection,
- Requires the implementation of 'secure by design,
- Imposes a duty of care for the lifecycle of products.

12.1.2 EU Digital Operational Resilience Act (DORA)

This piece of legislation specifically applies to financial institutions, but the key part of this for our purposes is that it also applies to any supplier of a financial institution, and it requires transparency within the industry and between financial institutions and their regulators. A high-level view of this legislation is that it:

- Imposes a framework of rules for financial institutions and their suppliers,
- Expands the scope of incident reporting, requiring faster reporting of incidents to regulators,
- Requires resilience-testing – all critical systems and apps must be tested yearly for resilience, as well as business impact analysis for 'severe disruption' scenarios,
- Imposes requirements on financial entities' contractual relationships with suppliers:
  - Suppliers must meet certain minimum requirements, with additional rules around outsourcing critical functions,
  - Financial entities should not rely on a single service provider for critical functions,
  - Critical suppliers must have a functioning EU subsidiary to provide services to financial organizations.
- Requires sharing of threat intelligence among financial institutions.

12.1.3 EU Network Information Security Directive 2 (NIS2)

An update to the earlier NIS directive, this legislation in essence requires member states to define what their Critical National Infrastructure (CNI) is, and then requires those entities and their suppliers to implement cyber security best practice. Possibly to avoid out-of-date and overly narrow definitions, the legislation refers to Critical Entities instead of CNI, and also defines Important Entities, which are digital service providers.

This legislation specifically addresses the digital supply chain, both by explicitly defining digital service providers/ suppliers as Important Entities within the meaning of the legislation and requiring the rules to apply to the digital supply chain of these Critical and Important entities, as well as the entities themselves. At a high level this legislation imposes the following:

- Each member state must define its Critical and ImportantX Entities:
  - Critical Entities essentially are a modern definition of CNI,
  - Important Entities are the many different types of digital service provider.
- Management bodies of Critical and Important Entities can be held liable for infringements and must both approve and oversee the implementation of risk management practices,
- Entities must implement measures to manage risks and minimize the impact of incidents,
- Entities must notify CSIRTs or a competent authority of an incident within 24 hours,
- Enforcement via big fines (up to 2% of annual turnover or €10 million, whichever is higher),
- Rules apply to the digital supply chain, as well as the entities themselves.

12.1.4 UK Proposal for Legislation to Improve the UK's Cyber Resilience

While the UK is no longer an EU member, a lot of existing UK legislation mirrors EU law. Therefore, the UK faces a similar issue to the EU, in that the flaws in the existing NIS legislation need to be addressed. As such, this proposed legislation is a similar update to NIS2, though it is currently only a proposal and only needs to apply to a single nation.

12.1.5 US Executive Order EO14028 – Improving the Nation's Cyber Security

While this US Executive Order technically only applies to the federal government, there are so many departments and agencies, and more importantly suppliers to departments and agencies, that the size and complexity of the modern digital supply chain means this will have a much greater knock-on effect. Requiring a greater focus on cyber security by the federal government and anyone who wishes to sell products or services to them will, essentially, force almost every large entity in the United States to abide by these requirements. In addition, this legislation specifically mentions the Zero Trust Model, a specific defense against, among other things, supply chain attacks.

The key points of this legislation are the following:

- Once again, enforces sharing information between the regulated entities,
- Requires incident notification to the regulators/authorities,
- Emphasizes the need for zero trust and mandates MFA and encryption,
- Requires baseline security standards for software sold to government, with a proposal for an Energy Star-type labelling of software as secure,
- Government-wide EDR,
- Software supply chain security:
  - Designate critical software.
  - Develop software bill of materials for products purchasable by government.
  - Provide guidance and tools on IoT security.

12.1.6 China Cyber Security Law (2016) Measures for Cyber Security Review (2020)

The Cyber Security Law of China contains a provision that Critical Information Infrastructure (CII) operators must go through a cyber security review if they obtain digital products or services that may threaten national security. This requires what are known as implementing rules, which define what the review measures are, and what CII operators are, and which were to be defined later. The Measures for Cyber Security review were defined in 2020 and focus on evaluating potential national security risks from a number of different factors.

This law has more of a geopolitical aspect, specifying that suppliers to CII do not obtain data or control and manipulate equipment illegally, and that they do not suspend product supply or technical support. However, among the defined factors in the measures are:

- Damages caused by supply interruption of products or services,
- The security, openness, transparency, and diversity of sources of the products or services, reliability of supply channels, and the risk of supply interruption,
- The measures are described as applying to:

  - Core network equipment
  - High-performance computers and servers
  - Massive storage equipment
  - Large databases and application software
  - Network security equipment
  - Cloud computing services
  - Other network products or services that may have significant impacts on the security of CII

The measures require terms and conditions in procurement agreements which will, among other things, require suppliers to cooperate in any cyber security review.