This is my (Tor Houghton's) unofficial English translation of our article on supply chain security that Rolv R Hauge and myself wrote for Telenor Norge's Digital Sikkerhet 2020 (this translation, version 1.01). All copyright original rights holder.

Notes: 1) A bunch of puns and references to "Musevisa" by Alf Prøysen don't translate very well, 2) Any use of "company" should be read as "organisation" and vice versa.

When nights are getting longer

Our national network is long and complex. When you stream the latest news broadcast from NRK [national broadcaster], an LED flashes intensely in a transport network node far down in the lower layers of the national network, to transport exactly your bits to you. In fact, a multitude of network components at various layers of the infrastructure such as, core network functions, service platforms and servers are involved, but you do not have to think about that when you watch Dagsrevyen [the news]. It just works.

The supply chains have become a bit like this as well. In a globalised and cost-optimised world, the chain of contractors and subcontractors are potentially very long and extensive. There are few, if any, companies that do "everything" themselves any more — or could do it if they wanted to. Behind almost every deliverable is an increasingly fragmented, complex, elongated and — unfortunately — increasingly less transparent network of partial- and sub-deliverables. This will probably remain the case in the foreseeable future.

By "supply chains" we include both services and products. They include both direct supply, that is, directly from suppliers and inputs, and indirect supply, such as subcontractors and their additional subcontractors and inputs. Subcontractors can also act as "super-contractors". This means that they provide deliverables on behalf of others, such as support and customer service. In understanding and assessing one's own supply chains, it is easy — and tempting — not to embrace their full breadth, and often significant depth. The delimitation must be related to the relevant threat picture, but it is no longer sufficient to only look at first-order suppliers; one no longer chooses a supplier, but rather an often extensive portfolio of suppliers.

From a security perspective, supply chains represent attack surface. Any business or person that contributes to a subcontract, and the deliverables of subcontract itself, provides an opportunity to influence security further up the supply chain.

This attack surface increases the likelihood of adverse operational incidents, whether they occur as a result of code vulnerabilities and inadequate handling of these, configuration errors, inadequate security hardening, successful personnel compromises, or just by plain accident and misfortune.

The longer and more fragmented the supply chain is, the further away the competence for handling incidents and means to positively influence their outcome.

And lakes freeze to ice

To meet this attack surface in an appropriate way, a company must first understand its own threat picture; and if one has customers, try to understand theirs. Businesses cannot do much about the threat actors themselves, but without insight into who and how someone most likely wants to influence ones business, it is difficult to choose the correct risk-reducing measures.

You need to know what values you and your customers possess — from the perspective of relevant threat actors — as well as their ability and willingness to carry out security-threatening activities against them.

Understand the values — for the threat actor

Most companies have an idea of what is commercially most important, by having already identified their “core business”, i.e. values considered most important from an economic perspective, or strategic assessments of where the business can add something unique. However, this does not necessarily provide the right focus and understanding of what represents the greatest “negative” values, those that have value for the threat actor. The business identification of core business often provides an incomplete picture of the activities and deliverables that require attention so as to minimise supply chain risk.

When security people refer to protecting the “crown jewels”, they see these from the threat actor’s perspective. What would have the greatest value for them — as a goal in itself or as a means to achieve their goals, a means to an end. That which represents the greatest value creation is not necessarily the thing — or only thing — that can inflict large losses on the business.

It may well be that your particular business, or that your “crown jewels”, are not priority goals for a threat actor. *The advanced threat actors are primarily looking for (more) information and access that cause them to reach, or get closer to, their actual goals.* Nevertheless, it is absolutely necessary to understand one’s own values, seen from the threat actor’s perspective, and as far as possible understand the same for the company’s customers. Although such a survey will never be be perfect, it is not possible to conclude that one is not a target.
In Digital Security 2018, we pointed out the importance of formalised collaboration with suppliers as well as important partners.

But for Norway — because everything we are and everything we have scattered over many, complex and long supply chains — hard voluntary work is also required. Every company must see themselves as part of the social machinery and take into account that they are both targets and vectors to a far greater extent than detectable values necessarily clearly indicate. The real target for the attacker may be someone completely different, and in this respect everyone should prioritise the most important security measures that support defendable ICT; the digital herd immunity which we referred to in 2019.

If everyone does “their part”, we will come a long way. By sharing knowledge of risk in complex and long supply chains, we will go even further.

Framing the risk assessment — understand and place responsibility

Supply chain risk is, based on the impact potential, a strategic issue for the business that requires strategic ownership. The choices the company must make in managing the risk often also have major consequences. This must be seen in a strategic perspective and dealt with at a strategic decision level. Not only are values at stake. The suppliers and subcontractors the company has chosen to expose itself to — and how well the handling of supply chain risk has been executed — can be decisive for which future customers the company itself will be considered a relevant supplier to. The customers that the business in the long run wants to be relevant to, and selectable by, is definitely a strategic matter.

The time perspective for the risk assessment must be seen in connection with the long-term benefit the company’s values will have for relevant threat actors, but also — and perhaps more importantly — how long-term consequences an attack through the supply chain can have on the company, its customers and society. The threat actors are persistently present, and to a large extent show ability and willingness to act over time.
Many organisations do not have their own expertise for this type of assessment, so one may have to seek help from a third party.

Mother mouse warns strongly (of a foul device)

The potential toolbox for risk reduction in supplier interfaces and supply chains is extensive. The toolbox can include everything from setting requirements, audit, instruments in the supplier relationship and in the company itself, as well as externally based instruments that may be relevant.

Requirements

To be able to identify relevant and good requirements towards a supplier, both security and — not least — domain expertise relating to the supplier’s business and the deliverable you receive is required. These are scarce resources, but insufficient competence in the role as purchaser is a common cause of inadequate requirements.

The use of references can simplify and ease the requirements process somewhat, and help to make the requirements more acceptable to both parties. Both laws and regulations, recognised frameworks and standards, industry norms, guidelines and certification schemes can be relevant references. This approach can also provide “automatic” maintenance of the requirements by developing and renewing the sources over time; in step with technology and the general threat picture. However, there is a need for competence in the requirements process to avoid disproportionate or irrelevant external requirements or certifications, which can have a negative effect on both the relationship, the cost level and the risk reduction achieved.

Requirements cost. Some requirements can cost a lot. The right risk assessment is therefore an absolute necessary prerequisite for requirements, negotiation of agreements and choice of supplier. The costs the company chooses to bear must correspond to the gain (risk reduction). Without a good understanding of risk, that balance is difficult to strike, and the choices are difficult to make.

Contractual requirements are often set at a relatively high level. To understand the risk reduction these requirements will actually provide, it will be important, especially in larger agreements, to clarify how the most central requirements will be met. This should be clarified before final supplier selection and conclusion of the agreement.

Further in the supply chain

Requirements in direct commercial relationships are important, but obviously not enough. It is our experience that security in terms of quality and improvement must be driven by demand from the buyer, and a certain willingness to pay for security and risk reduction. A requirement that the supplier must impose the security requirements further on to its subcontractors is one tool for giving security requirements a demand-driven effect further down the supply chain. In general, it is also important to set requirements for control of received deliveries.

Many companies investigate matters related to potential suppliers, but few demand transparency into who their subcontractors are. The ability to document this effectively will often depend on the supplier's management and reporting systems.

Skewed balance of power in supplier relations

All companies will from time to time need to enter into supplier relations where the balance of power is anything but even. A meeting between large multinational service providers and an average Norwegian small business will often give the latter little room to make special demands. It becomes all the more important to familiarise oneself thoroughly with the conditions offered, choose the supplier on the basis of identified risk, ensure that the deliverable is used correctly and in line with security instructions from the supplier, and maintain a reasonable degree of control over the delivery's security quality. The latter may appear resource-intensive, but many large suppliers where the conditions are basically indisputable, will still — if for no other reasons that commercial — offer their customers documentation of independent control of security quality in their deliverables.

In the absence of the opportunity to make demands, an organisation must simply consider — given the conditions — whether the chosen supplier is the right one. Dissatisfaction with the conditions or the security quality must be communicated by choosing or switching to an alternative supplier; thus exercising market power.
In the face of a strongly desired, and strongly positioned, supplier who will not accept an organisation's requirements, it is important not to incur unknown risk by resigning without assessment of reality. The discrepancy between the company's requirements and the supplier's offered conditions should be systematically identified and used in the assessment of supply, supplier and supply chain risk. Only when this risk has been assessed and known

can the organisation make an informed decision as to whether the supplier constitutes an unacceptable risk and how the risks can be managed if an agreement is nevertheless entered into.

Control

Many people associate "control" with something one does postact. But there are good reasons to check suppliers both before and after entering into a contract, and definitely before the security incident is a fact. Depending on the risk the supplier and the deliverables are considered to represent, and how decisive the requirements are for the risk to be acceptable, control in the form of company review ("due diligence") may be appropriate even before the conclusion of the agreement.

For most, the main emphasis will still be on ongoing and/or periodic control activities within the framework of an ongoing supplier relationship. This can be exercised in several ways and to varying degrees; for example by:

- **control of the actual delivery**

  This includes all forms of security-relevant quality testing, including offensive security testing.

- **inspection and audit**

  These are resource-intensive activities that will have to be prioritised towards suppliers and deliverables that represent the largest attack surface/risk to the business.

- **reporting and self-reporting**

  Although these do not provide the same insight as a stand-alone first-hand inspection, they may provide relevant transparency in a cost-effective way.

For many organisations, it will be relevant for both competence and capacity considerations to use third-party assistance — that is, yet another supplier — to assist in such activities. Full service outsourcing can be challenging, however, as control activities often also require specific domain expertise from the organisation itself.

Exercising first-hand control several stages down the supply chain is not only challenging to gain access to, it also entails increased use of resources. If such control is relevant, this should be reserved for selected subcontractors/deliverables that pose a particularly high security risk. It is more realistic to demand confirmation that control has been exercised in each link down the supply chain, as far as relevant. With society’s increasing attention to supply chain risk, many companies must expect increased demands for documentable exercise of control over their own supply chain, both from the authorities, through certifications and approvals, and from larger risk-exposed customers.

- **Understand** what is valuable, to you, to your customers and to relevant threat actors
- **Understand** and place responsibilities, and anchor responsibilities and risks at the strategic level
- **Understand** the supply chains, and demand insight into them

- **Set** risk-based requirements, set requirements for continuation in the supply chain and exercise control
- **Find** the right balance between control of supplier, subcontractor and received deliverable
- **Provide** positive commercial incentives for good security and good security interaction
- **Seek** to shorten supply chains and reduce the need to expose values to them
- **Equip** yourself to deal with supply chain attacks — separate and segment where you can
- **Ensure** necessary in-house competence, ability and capacity to understand, assess and validate, including security test, your suppliers and their deliverables.

Instruments and supplier relationship

The choice of supplier is one of the most fundamental tools in the toolbox for reducing and managing supply chain risk. The preference should be suppliers who understand the organisation's threat picture and risks, and show the ability and willingness to act on their own in line with these.

Penalties and fines

In agreements for larger and complex deliverables, it is considered good hygiene to make room for negative measures if requirements are not met. In addition to legal authority to withdraw from the agreement, punitive measures are usually of a financial nature. They do not necessarily give, for all consequences of a security breach, full recourse against the supplier. On the contrary, we see repeated examples of financial instruments not being commensurate with the risk and damage caused by inadequate compliance with requirements; some suppliers see themselves better served by paying "penalties" than actually delivering. The purpose of this tool is not achieved when it does not lead to real behavior change. A credit note on cheaper services in the next quarter is a meager consolation, if at all relevant, in relation to the risk the business incurs and any losses it suffers in the event of incidents.

We are familiar with companies that carry out both pre-contractual and annual inspections of their potential suppliers, including auditing activities. Those who fail such an audit at the first attempt and do not improve sufficiently for a soon-to-follow second audit, are placed in quarantine, are at risk of losing their existing deliverables by the organisation initiating re-sourcing, and the supplier is deprived of the opportunity to offer their other products and services to the business for an extended period.

Positive incentives

We see relatively rarely — probably too rarely — that positive measures are used to stimulate compliance with requirements, risk reduction and good security work at the supplier. All large and complex deliverables have a significant degree of risk; a risk the customer often makes significant financial provisions to cover. Given that it is almost without exception more cost-effective for both parties that delivery is performed with the right security quality than using risk provisions for compensatory measures afterwards, it is

surprising that bonuses are not more often set up promote correct delivery — where the customer accepts that this is one possible application of the risk provision and part of the price picture.

Positive incentives help to cultivate a positive, strong and good supplier relationship. Willingness to interact and to go “the extra mile” for each other, gives a far greater probability that the supplier:

- is willing to do a “little bit extra” and be proactive in addressing risks beyond contractual requirements and/or without each contribution having to be treated commercially;
- contributes to good and efficient incident management also towards its suppliers and further towards their subcontractors in the event of incidents; and
- on its own initiative seeks improvements and proposes changes that contribute positively to the customer’s risk picture; a risk picture the supplier perceives to have a degree of ownership of.

The supplier relationship will not only be characterised by the commercial framework, but also by the ongoing management driven by the organisation’s own internal KPIs and incentives. There may therefore be contradictions between the requirements and expectations set for a supplier, and the operational delivery interface the company has with the supplier. To avoid this, internal incentive models should be reviewed and adjusted so that they conduct the desired behavior in relation to supplier and supply chain selection.

Shorten the supply chain

Despite the intention, willingness and a certain ability to implement the measures we have discussed so far, it is obvious that the residual risk increases the longer the supply chain is. Choices that help to shorten the supply chain are therefore a natural part of the company’s toolbox of risk-reducing measures.

The ability to simply do more for oneself, within the framework of one’s own business and direct control, has in the short term a number of obvious limitations, both financially and competence-wise. The time perspective is important, and we claim that the ability to implement such measures is often underestimated with a short-term perspective, instead of being considered as long-term investments and improvement plans.

In areas where the organisation has identified a significant risk of security-threatening impact through the supply chain/deliverable, long and extensive underlying supply chains should have a significant negative effect on the risk assessment and influence the choice of supplier.

Strengthen the ability to influence through community

Influence by seeking fellowship with other businesses has both negative and positive sides.

The power relationship between customer and supplier can be changed directly by several customers with the same needs forming joint purchasing companies. In the telecom industry,

the purchasing alliance BuyIn is one such example; it was started as a joint venture purchasing organisation for Orange and Deutsche Telekom, and has since gained seven additional members. However, such constructions are a double-edged sword, partly because:

- they in themselves constitute an extension of the supply chain;
- they in some cases serve customer businesses with significantly different threat and risk picture, and risk appetite; and
- they can distance the purchasing function and the choice of supplier from domain competence of the deliverable, which is, among other things, critical for the correct requirements and control of the deliverable.

A more neutral form of influence can be realistic to achieve through industry and trade organisations in which both the customer and supplier participate. The room to maneuver within such a framework ranges from the completely non-binding culture-building, via norms, to de-facto standards, certifications and binding multilateral charters. All of this can and should affect security in the supply chain, not just the deliverable. Customer companies that do not themselves have the capacity for such active participation and advocacy work should also find out about relevant industry organisations and their norms, standards, certifications and charters, and the extent to which these address the supplier and the security of the deliverable. Preference for suppliers who have joined and/or actively participate in such, and preferably reflect a similar expectation towards their subcontractors, is often a good indicator of reduced risk.

Strengthen the suppliers

It is our experience that communicating the threat picture in a way that makes it understood, the ability to manage risk well assessed by the supplier himself and necessary changes taken into account when the offer is made, can be very challenging. In order to be able to expect the supplier to have the best possible understanding, it is important to use time and resources in the dissemination work before choosing a supplier and entering into a contract.

The reality after entering into a contract may deviate from expectations, even contractual requirements — regardless of whether or not the expectations were realistic and the requirements understood. For any long term relationship, it is important that the customer is willing to invest in further dissemination work and strengthening of the supplier's competence. This should be seen as good investment in very cost-effective, risk reducing, measures.

From the supplier's point of view, it can be difficult to understand, and keep pace with developments in, their customers' threat and risk picture. Thus we must soberly assess the need for, and calculate the use of resources in, lifting our suppliers in critical areas such as competence and knowledge of each other's organisation and business. Together with the supplier, through measures such as training, their personnel can be put in a much better position to understand their customer's threat picture. This increases the probability of delivering in a security-acceptable manner, good interaction when handling incidents,

deliverables of satisfactory security quality and not least that suppliers act with the same competence towards *their* suppliers, down the supply chain.

Joint exercises in incident handling can provide great benefits. Not only does it help to strengthen the parties' ability for future incident handling, but also to identify weaknesses in interfaces and interaction. Exercises also strengthen personal relationships and mutual competence development about business, infrastructure, strengths and weaknesses.

Instruments in your own organisation

There are several types of measures that can be taken in one's own organisation that reduces the risk associated with a supply chain's attack surface. Whether you can implement these measures yourself, or need help from another supplier, depends, among other things, on the organisation's competence, capacity, understanding of its own IT and participation from first-tier suppliers. Some measures will affect the probability of the risk occurring, while others will reduce the extent of the consequences.

Segregation, segmentation and access

Segregation, or separation, is a category of security measures which, by ensuring that traffic is not allowed to flow freely between systems and system components, adds detection capability, supports access control and differentiated access, adds several layers to the security model, strengthens the ability to handle incidents and — not least — contributes to limit the consequences of a security incident. The mechanisms used (infrastructure, virtualisation environments, storage and support services that are not shared across exposure requirements, micro-segmentation versus large networks, shared components, access control and authentication mechanisms), as well as the business and process architecture, sets the premise on how strong this segregation can be and how effective it is.

Restrictions on access and access rights are particularly important in supplier relationships that form supply chains. Often — in our view, too often — extensive access is expected related to the supplier role. This appears to have many causes, such as a business model based on the customer not having competence themselves, inadequate security competence, naivety and unfounded trust, cost focus or old habit. There is a great security gain in adapting the delivery model to greater competence in one's own organisation, where, for example, requirements for documentation from the supplier and that employees receive relevant training can contribute to reduced supplier dependence and access requirements. Several companies must dare to challenge their suppliers by asking questions to statements such as "we just have to have it" and "everyone else thinks it's okay" when suppliers demand access. The way suppliers expect to exercise access is often simple, uncertain, old-fashioned and characterised by a naive expectation of blind trust. Some suppliers also want us to expose our systems and infrastructure through *their* remote access solutions.

In Telenor Norway, we strive for all third-party access — in addition to being legal — to be:

- limited to the actual need for access to information, function and level

- limited to the actual need for duration, including also avoiding permanently active rights by using disabled accounts for future and short-term needs (error correction, support)
- under our own real management and control
- subject to proper security monitoring
- exercised in a technically secure manner in relation to, among other things, communication security, authentication and avoiding continuous connection to information and values

The above does not always meet the expectations of all our suppliers, but is considered necessary for having sound security. Access control and authentication must be applied in several layers; not only in the access solutions, but also closer to each individual service; furthermore, the infrastructure must be able to enforce this access.

Supplier access — in the extreme case only in emergencies when our own competent personnel fall short—- this can be impossible to eliminate without disproportionate operational risk. However, with the facilitation of deactivated access rights, a sound way of exercising access, and good processes for “emergency activation”, the supply chain risk can be reduced much within the framework of acceptable operational risk.

Segregation of infrastructure, services, information-bearing systems and vital components in the access infrastructure are significant measures to reduce the risk of both our own personnel and our suppliers' access. Unfortunately, there are many examples — especially in the last five or six years — of supply chain attacks where supplier end-user equipment or other infrastructure is compromised and used to gain access to customers through the supplier’s accesses [e.g. Operation Cloud Hopper, Operation ShadowHammer].

Reduce exposure

It can be easy to look blindly at the question of “access or not” based on the assumptions that already exist. Techniques and measures for reduced exposure of both components and information are many and situational. It is a valuable exercise to return to the need for exposure and analyse the scope for minimising it. This can reduce the risk score, and hence the need for other, more resource-intensive measures:

- Does the *whole* system with all its functions need to be exposed on an equal footing, or can it be split up and thus give it a more limited exposure?

- Does this dataset need to be exposed in *its entirety and in full detail*, or is it sufficient for the purpose if only a subset is given access, to a reduced level of detail, or to a modified dataset where sensitive elements have been removed or one-way transformed?

Hand over or give access?

Provided that one has good access control, good opportunities to enforce it, and robust access mechanisms, there could be large differences in the risk exposure by providing access to information versus handing it over. However, the possibility of preferring access

over handing over the information seems to be gradually reduced, as deliverables in all stages increasingly include information processing and production using tools and systems outside one's own business, often also the outside supplier's.

[image showing graph of supply chain complexity]
In understanding and assessing one's own supply chains, it is easy — and tempting — not to embrace the full breadth, let alone the often significant depth.

Multiple suppliers

Multi-supplier procurement strategy is often referred to as risk-reducing measures in relation to delivery risk. From an operational continuity perspective, the effect may appear obvious; if one fails, the business can still get deliverables from the other. From a security perspective, however, it is a double-edged sword. Doubling suppliers in an area can lead to a doubling of the related attack surface. Multiple suppliers in a technology segment will in many cases increase complexity, which in itself has a negative impact on security. On the other hand, multiple suppliers in a technology segment can give increased freedom of action to quickly switch out one supplier in the event of (serious suspicion of) security incidents, or in the supply chain behind.

Operational and security advantages and disadvantages of multiple suppliers in a technology area may thus have net gains, but must be carefully considered against the relevant deliverable.

Deliberate splitting of deliverables between multiple suppliers may provide relevant risk reduction in several ways; among other things because it supports minimisation of the access and information requirements of the individual supplier, as well as supporting segregation and segmentation. This is a proven methodology from organisations with a great need for and focus on confidentiality; where few are given broad access and the opportunity to understand the whole. This is not only relevant for national security interests, but also for high-value business-critical information such as intellectual property. In relation to supply chains, the integrity perspective can also be very central, but even there, such supplier and delivery segmentation could have an effect.

Competence, capacity — and tools

We have previously mentioned the need for competence and capacity for, among other things, requirements and control. The big IT outsourcing wave gave many companies expensive experience by underestimating the resource requirements and the importance of competent operation of the supplier interface.

The same effects will necessarily increase — if one is to strive for follow-up and control to keep the risk down — as the scope, complexity and depth of supply chains increase. Although this cannot be compensated with requirements, control and follow-up capacity alone, the increasing need for resources to perform risk mitigation should be weighed

against alternative resource use — for example by keeping several risk-bearing activities under direct control in one's own business.

Competence and capacity — and the authority one may have acquired to exercise control — can fall short without tools. Administrative tools that support management systems for supplier follow-up, with systematic recording of observations, reporting, control and other assessments are valuable and increasingly necessary as one acquires insight and starts acting actively towards a gradually larger part of the subcontractors who are identified to contribute to security-critical deliverables.

Among technical tools, several types may be relevant. Whether the organisation has special contractual access to in-depth vulnerability scanning or not, automated tools for vulnerability scanning may also have legal application against suppliers' and subcontractors' visible infrastructure. The organisation's own or its security service provider's service(s) should be able to be instrumented with relevant searches related to important deliverables. Both in a pre-contractual phase and in an ongoing delivery, placement of the company's security monitoring, such as sensors, in dedicated parts of the (sub)suppliers' infrastructure may be a relevant measure to strengthen the supplier's security understanding, deter potential insiders and provide increased transparency and thereby strengthened ability for control.

Security testing

The term security testing embraces all verification of the deliverable's integrity and its ability to maintain confidentiality and availability. It is a very broad toolbox of techniques and approaches, spanning both technology, people and processes. It is necessary to look at security testing, like other security measures, in a holistic context across the digital and physical domains.

We will scratch the surface a little of this comprehensive topic.

About security testing

Verification of security, to exhaustively prove that something is "safe" is for most cases and businesses insurmountable, and definitely disproportionate. Most forms of security testing are time- and resource-limited activities.

Security testing should at least aim to identify obvious errors that relevant threat actors can be expected to exploit. Remember that advanced threat actors have far more time and resources, and sometimes better conditions, to find vulnerabilities than the company and its competent suppliers of security testing can afford within risk-proportional limits. A security test without serious findings therefore never means that there can be no exploitable vulnerabilities in the deliverable. Nevertheless, it is of great value to find and close "simple" vulnerabilities, so that the threat actors are forced to use greater resources and more advanced methods.

Security testing must include "negative testing", i.e. actively searching for and trying out what should not be possible. This requires knowledge, imagination and the ability to think like a

threat actor, and a relevant scope — which will often span beyond and across the individual deliverable.

The specific device for security testing largely depends on the type of deliverable in question (software, hardware, services, people) and how it is delivered (service-based, made available; versus handed over). Relevant forms of security testing should take place both as an integral part of the supplier's development process, the finished deliverable, at delivery receipt and periodically throughout the deliverable's life cycle. The latter can take into account, but should not unilaterally focus on, the frequency of change of the deliverable, as the environment (technology, threat actors, application) is also changeable.

Through the supply chain

It is our experience that security testing of received deliverables will also have an educational effect on the supplier. Despite the fact that the deliverable has a commercial framework that may have inadequate means to impose improvement, most suppliers will have a genuine desire for improvement. Commercial instruments can strengthen the incentives for improvement, but with good intentions connected with a culture of, and strategic ambition for, security quality, there follows a willingness to act. This phase will often highlight whether you chose a supplier that has a consistent understanding of threats and risks.

Just as important as setting requirements down the supply chain for relevant security testing is verifying it and using the results. The company should — as far down the supply chain as is relevant and feasible — require more than just confirmation that relevant security testing has been, or is being, performed. It must be documented *who* did the test, *what* they tested, *how* they tested, *when* and on which version of the deliverable the test was carried out. A description of what *findings* were made, what *risk* the findings are considered to pose and last but not least, what will be *done* with the findings must not just be a statistical summary or limited to critical findings. The mitigating controls must also be documented with *who* has performed, *what*, *when* and *how*. Such transparency and verification of security testing and follow-up of findings is not only a control mechanism to ensure that adequate security testing and follow-up takes place, but also supports the organisation's risk assessment, and better enables it to identify requirements for mitigating controls under its own auspices, including also adaptation of its own security testing. Where continuous/frequent security testing is also integrated in development or production processes, it may be relevant to require access through read access to tools or reports.

The attack surface of the deliverable is not limited to components and input factors that are directly included in it, but also includes the surrounding technology, processes and people of each player in the supply chain. In assessing the need for and control of the implementation of security testing, it is therefore essential to require not only security testing of the deliverables, but also of suppliers' technology and processes in general.

Vulnerability management

From the supplier's side, a need for confidentiality about vulnerabilities will often be invoked. This can be legitimate and in the interest of all parties where the deliverable has already

been deployed, when a relatively short time since the vulnerability was identified, the vulnerability is not widely known, the vulnerability is not actively exploited and there are many customers who have used the deliverable. Although it is easy to suspect confidentiality about vulnerabilities to be commercially motivated, there may be, *for such cases,* a highly justified risk balance in relation to the harmful consequences of information sharing.

A large part of the benefits from security testing — both the organisation's and the suppliers' — are linked to the suppliers', and supply chain's as a whole, ability to handle timely vulnerabilities. There is a case for making a risk-based prioritisation of which vulnerabilities are to be fixed (first), but we unfortunately all too often see narrow or optimistic risk assessments, incorrect assumptions and assumptions about the deliverable's operating environment and use scenarios, and a rejection of "Low" and "Medium" vulnerabilities as categorically unimportant and less dangerous. Vulnerability management — like lifecycle management in general — is a key part of setting requirements to the supplier, and must be an ongoing activity in the entire supply chain that results in technology-based deliverables.

Some vulnerabilities, often in deliverables that have a long development cycle, long life cycle and of a permanent nature, such as hardware components, will still have known (and unknown) vulnerabilities that cannot be remediated without replacement. Replacement, possibly accelerated periodic renewal, must of course be considered as a mitigating control, but it is unfortunately the case that we are all constantly exposed to a number of known vulnerabilities, without having good alternatives and opportunities to avoid them. Recent years' reports of serious errors in processor architectures [VoltJockey, Spectre/Meltdown,Foreshadow]] as a result of constant pressure to deliver performance are examples of this. These must simply be taken into account in the way the deliverable is structured and used, and/or be met with compensatory risk-reducing measures in the form of preventive and revealing controls.

Provably secure? Provably malicious?

The debate about supply chain security has in recent years increasingly included national security interests. The risk of various forms of participation from, or undermining of the security of suppliers operating under other political, societal and legal conditions is actualised.

Especially within technology deliverables, there will always be several vulnerabilities, both observable and unidentified, and it will not be possible to test oneself to a conclusion about absolute security. Likewise, it is almost impossible to determine with certainty whether an exploitable vulnerability is an instance of lack of quality or deliberately placed by, or on behalf of, a threat actor.

External instruments

Supplier Intelligence

To help assess the many suppliers that are revealed in the supply chain survey, there is a relatively rich market of third parties who can assist an organisation with supplier assessment, profiling and information gathering. There are products that are based almost exclusively on open information, but also products and services where information is

obtained from less accessible and partly unclear sources. This knowledge has value as a basis for risk assessment in the selection of suppliers, and in ongoing risk management as suppliers change their subcontractors, and thus their risk profile.

Managed Security Service Provider
In recent years, there has been increased recognition of the supply chain as an attack vector, both through deliverables and access provided to suppliers. The supplier's security level — among other things in relation to good security monitoring, and hence the ability to detect both compromise of its own infrastructure and attacks from its subcontractors — is therefore crucial for the customer's security. For many suppliers, especially the smaller ones, however, it will not be realistic to establish strong security monitoring solely with their own resources, and it may be appropriate to set requirements that the supplier uses, or otherwise meets high requirements for security monitoring by using, services from a Professional Security Service Provider (MSSP).

Incident Response Retainer
As with security monitoring, it is unrealistic for almost any business to expect that the supplier, or the business itself, to be able to handle a successful cyber attack with extensive compromise from an advanced threat actor on its own. It is quite common to need specialist assistance for such incident handling, but how quickly one can get such assistance and how expensive it will be depends on whether one has entered into such assistance agreements in advance. By entering into such an agreement, making these demands in particular to suppliers with a large identified potential for damage, and recursively to their subcontractors, the risk of long-term, extensive consequences for the business by successful compromise of the supplier is reduced.

We must avoid the mouse trap

It would be misleading to end with optimism here. Everyone falls into the trap — it's just a matter of time. It is good to take care, so it happens as rarely as possible and with as little damage as possible, but there are many traps out there.

We have to do what we can to make it all the way to the next Christmas Eve — and the one after that. It is just as important to plan to fall into the trap as it is to avoid it. In this article, we have highlighted a toolbox of both preventive and harm-limiting measures, and the need to choose risk-reducing controls based on risk identification with a correct understanding of value, threat and risk. Without a genuine recognition that supply chain risk, given enough time, will materialise in incidents against the business, this work cannot be framed correctly.

Finally, when other risk-reducing controls have been exhausted, the organisation must choose where and to whom it wishes to expose its supply chain residual risk.

<end>