‘Where did my technical data go?’ The legal nexus between export control obligations and cyber security vigilance

A release of technology subject to export controls following a cyber attack may trigger a range of liability and reputational issues as well as reporting obligations. Tamer Soliman, David Simon and Gretel Echarte Morales offer guidance on how best to prepare for what some are calling ‘the inevitable’.

One of the most significant emerging issues facing companies considering their cybersecurity exposure is the potential liability risk associated with the loss of export controlled technology in a cybersecurity attack. In addition to compliance with data protection and data privacy obligations, the potential release of technology subject to export controls may also trigger reporting obligations, potential liability and broader reputational issues under export control laws designed to regulate the transfer of sensitive commercial, dual-use and defence know-how to foreign persons and entities. In recent years, the intersection of cybersecurity, national security and trade control regulation has increasingly come into focus, and has resulted in a number of regulatory developments and proposals, including the use of sanctions to target persons and entities engaged in malicious cyber activities, efforts to regulate exports of offensive cybersecurity and cyber surveillance tools, and efforts to address the protection of unclassified export controlled data stored or transmitted electronically.

This article focuses on an emerging, and largely overlooked issue at the intersection of the export controls and cybersecurity. For companies considering their legal obligations and risks relating to a potential cyber intrusion, the chaos and potential liability concerns generated from an attack may be potentially compounded by the exfiltration of controlled technical data that ends up overseas or in the hands of a foreign person in violation of export control laws. For both planning and risk mitigation purposes, it is important that cybersecurity assessments and response plans reflect an understanding of how these laws may impact regulatory risk, and potentially create reporting obligations. This article addresses the potential bases of exposure, as well as key areas of ambiguity and associated reporting obligations arising from the compromise of export controlled technology in a cybersecurity attack.

US export controls

By their terms, the prohibitions of US export control laws define ‘exports’ in terms that are broad enough to implicate both potential liability exposure and positive reporting obligations in the context of a cyber attack involving releases of export controlled information, without comprehensively setting out consistent requirements or ‘safe harbor’ provisions for the protection of such data. Setting aside criminal penalties that may be imposed for wilful violations of US export control laws, significant civil and administrative penalties under these laws apply on a strict liability basis.

The International Traffic in Arms Regulations (‘ITAR’), administered by the US Department of State, Directorate of Defense Trade Controls (‘DDTC’), govern the export of defence articles and services, including the technical data relating to controlled defence hardware and software. The Export Administration Regulations (‘EAR’), administered by the US

Department of Commerce, Bureau of Industry and Security ('BIS'), govern technology relating to the development, production or use of commercial/dual-use items. Subject to important differences, as discussed further below, both define the term 'export' extremely broadly. The Department of Energy ('DOE') regulates the export of technology relating to special nuclear materials and the Nuclear Regulatory Commission ('NRC') regulates the export and import of nuclear reactors and other nuclear facilities, related assemblies, equipment and components.

As a threshold matter, exports of controlled technology across these different regulatory regimes can occur in physical or intangible form, including through electronic transmission, the provision of network/server access, or otherwise when information is 'released,' sent or taken abroad. A 'release' of technology can occur through visual or other inspection that reveals technology or through oral or written exchange of such information. Whenever such an export/release of controlled technology occurs, authorisation is required, either in the form of a general or specific licence, depending on the country, end use, and end-user involved. Even the domestic release of controlled technology to a non-US person is 'deemed' to be an export/re-export to the country of the person's nationality.

Of these various export control regimes, only the EAR excludes from the definition of export the sending, taking or storing of EAR-controlled technology in encrypted form under certain circumstances. In particular, the exclusion provides that these terms do not apply to sending, taking or storing technology or software that is:

i) 'unclassified';
ii) secured using 'end-to-end encryption';
iii) secured using cryptographic modules compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other procedures that are in accordance with US NIST publications; and
iv) is not intentionally stored in a country listed in the regulations as a 'Country Group D:5' country, a list of countries that includes, among many others, China and the Russian Federation.

The EAR define 'end-to-end' encryption for these purposes as data that is not in an unencrypted form between the originator and the intended recipient, and the means of decryption have not been provided to a third party. Encrypted data that does not satisfy these criteria may be ineligible for exclusion, and therefore may constitute an unauthorised export.

Companies should be aware of circumstances where the export control laws may require mandatory reporting where export controlled data has been released/transferred through a cybersecurity breach.

Moreover, the agency has taken the position that, absent other facts, the victim of a hack or other security breach of EAR-controlled data that meets these standards will not generally be liable for the unauthorised export in the absence of other facts. The agency caveats this position on the premise that the victim did not provide access information or otherwise allow the unauthorised person to gain access to the encrypted data by making such access available having 'reason to know' under the circumstances that the system would be breached or data would be exfiltrated. Accordingly, while this language provides a helpful basis for defence, it still leaves room for a circumstantial evaluation by enforcement officials of the reasonableness of the company's actions leading up to (and potentially in response to) the breach and its mitigation. Moreover, companies should ensure that any end-to-end encryption satisfies the standard set forth above before relying on the exclusion.

Notably, neither the ITAR nor DOE's export controls on technology relating to special nuclear materials include a similar exclusion. DDTC considered adopting for ITAR purpose the end-to-end encryption standard adopted by BIS in a proposed amendment to the ITAR, but withdrew that aspect of the rule pending further consideration. The timing and content of a subsequent proposed rule for ITAR technical data remains to be seen. Until then, the treatment of technical data in connection with potential breaches remains subject to potentially divergent regulatory interpretations and approaches of the agencies. Companies should expect that the release of controlled technical data through a cyber attack on a company's networks may lead to scrutiny of their cybersecurity safeguards. Consequently, it is important that those safeguards be based on a risk assessment and be consistent with any applicable safeguard standards (e.g., NIST SP 800-711) that either apply by regulation or contractual obligation, or that otherwise serve as reasonable and appropriate benchmarks, as discussed further below.

In addition to safeguards, companies should also be aware of circumstances where the export control laws may require mandatory reporting where export controlled data has been released/transferred through a cybersecurity breach, as well as when agency practice and the circumstances may make a voluntary disclosure an advisable consideration. Depending on the circumstances, there may be a positive obligation to disclose the release of ITAR-controlled technical data to the government. Although companies may have the option to

'voluntarily' disclose ITAR violations in other contexts, Part 126 of the ITAR requires companies to promptly disclose the release of ITAR technical data to a number of countries subject

US sanctions laws and cybersecurity breach considerations

The United States has recently turned to its economic sanctions laws as an additional tool to target 'malicious cyber-enabled activities' and their perpetrators. The sanctions laws, administered by the Treasury Department's Office of Foreign Assets Control ('OFAC'), impose broad prohibitions on transactions, including but not limited to, exports and re-exports of technical data, involving certain sanctioned countries or parties on a strict liability basis. Executive orders 13694, 13757, and 13687 provide for imposition of sanctions, including an asset freeze and broad prohibitions on virtually any activity, involving persons deemed to be complicit in or to have undertaken malicious cyber activities that harm various US interests. OFAC has designated a number of entities as subject to comprehensive asset-blocking and reporting requirements based on malicious cyber activity under these authorities. More broadly, the US maintains comprehensive embargoes and other trade sanctions against a number of jurisdictions (including, but not limited to, Iran, Cuba, Crimea, North Korea, Russia, Sudan and Syria) as well as a persons and entities designated by OFAC.

As with the export control laws, US sanctions establish a basis for strict liability penalty exposure against companies whose data has been exported or transferred to prohibited countries or parties. The release or transfer to a sanctioned country or person of anything of value (including proprietary information) without authorisation constitutes a violation of the sanctions laws subject to penalties on a strict liability basis. Certainly, even taking into account OFAC's notoriously broad discretion, it would be perverse and run counter to the purpose of the cybersecurity executive orders referenced above to penalise a purely passive victim of the very same cyber criminal that is targeted by the sanctions.

However, a consideration of other fact patterns involving potential cyber attacks brings into light some potentially significant, and largely overlooked, risks companies may face in practice under the sanctions laws. For example, consider a scenario involving a ransomware attack against a large company, in which the attacker seeks payment of a ransom in exchange for refraining from action that would damage the company's interests. What if the attacker is listed as one of the parties designated by OFAC for malicious cyber activities?

In a number of analogous cases involving ransom contexts targeting companies with deep pockets (from Somali piracy to South American narco-traffickers), OFAC has, for policy reasons, taken the position that the sanctions laws prohibit payment to the sanctioned criminal extortionist without authorisation (which it may or may not provide). In practice, it is critical that the company carefully manage its discussions with the agency in a manner that navigates these issues in parallel with its management of the potential compliance risk as well as the significant commercial and reputational risks associated with the ransom demand. To make matters worse, under the agency's long-standing 50% rule, even if the entity demanding the ransom is not designated, but is owned at least 50% by a designated party, OFAC considers the entity to be a sanctioned party subject to its sanctions prohibitions. Outside the designated party context, if the company has determined that the ransom demand is coming from a person in an embargoed country, or acting on behalf of the government of that country, similar issues will arise. The more the US turns to its sanctions laws as a tool in its arsenal to target government and non-government perpetrators and sponsors of malicious cyber activities, the more important it is that companies understand and take these issues into account in their cyber incident response planning and response activities.

to arms embargo (or their nationals). Where a breach is determined, or reasonably suspected, to involve one of these countries, mandatory disclosure requirements are implicated.

Similarly, the DOE has adopted the position that a company that becomes aware of a technology transfer that violates the requirements of its regulations must notify the department within 30 days of becoming aware of the violation. In addition, companies who have exported controlled technical data under export control licences, technical assistance agreements ('TAAs')and other authorisations may be subject to conditions and provisos that impose reporting requirements in connection with unauthorised release, transfer or other export of controlled technology that could be implicated in the event of a breach. Regardless of potential liability for the underlying release, failures to report constitute independent violations of the regulations under the circumstances described above.

While the considerations above apply to any party who holds export controlled information, there are also obligations to safeguard and report cybersecurity breaches for government contractors and subcontractors to the Department of Defense ('DoD') – 'Covered Contractors' – who process, store or transmit 'covered defense information,' including unclassified export controlled technology and technical data in relation to those contracts.

Covered Contractors are subject to strict cyber safeguarding and positive reporting obligations pursuant to the DoD's final rule adopted in October 2016. The DoD's definition of 'covered defense information' includes unclassified export controlled information (including dual-use, ITAR, and sensitive nuclear technology information) that is collected, developed, received, transmitted, used or stored by or on behalf of the contractor in performance of a DoD contract. In addition to complying with certain cybersecurity standards, the final rule imposes on Covered Contractors an affirmative duty to report cyber incidents to the DoD within 72 hours after they are discovered when covered defense information is compromised.

Finally, setting aside mandatory disclosure requirements, companies should also consider whether voluntary disclosures of potential violations are in its interests. In the absence of a positive obligation, this is a highly case-specific determination that should be informed by the facts and circumstances, including the issues raised by the breach and their potential impact on the national security and foreign policy considerations underlying the particular export controls involved, as well as an understanding of the enforcement practice and approach of the agency.

Integrating export controls into cyber preparedness and response plans

As the above suggests, lack of knowing or wilful conduct, and indeed status as the victim of a cyber attack, is not an affirmative defence to liability under the export control and sanctions laws, although it is typically taken into

account in determining whether a monetary penalty is appropriate in light of other mitigating and aggravating factors in the case.

As a practical matter, in the event that such an incident were to come to the attention of the agencies, enforcement officials would not likely pursue enforcement action under such circumstances in the absence of an indication that the company failed to take reasonable measures either in its prevention of the incident or its response upon discovery. Moreover, apart from the underlying breach, the facts and circumstances of the breach may give rise to positive reporting obligations to one or more of these agencies. The failure to identify, assess and comply with this potential reporting obligations may lead to additional penalty exposure even if the circumstances of the underlying breach would not otherwise have been viewed unfavourably.

Whether an organisation has already a cyber incident response plan in place, or is creating a new one, export controls issues should be addressed.

Accordingly, to mitigate the risks of regulatory enforcement by export controls agencies, organisations of all kinds should adopt the necessary measures, policies and procedures to protect their controlled technical data based on best practice from both a cybersecurity and export control perspective. Whether an organisation has already a cyber incident response plan in place, or is creating a new one, export controls issues should be addressed. The 'Best Practices for Victim Response and Reporting of Cyber Incidents' and the 'National Cyber Incident Response Plan' published by the Justice Department and the US Department of Homeland Security ('DHS'), respectively, provide useful starting points when crafting a cyber incident response plan.

Identifying and mapping controlled technical data

Without a clear understanding of whether and how its information is exported, by which export control agenc(ies) and subject to which licensing requirements, the company may not be in a position to readily determine whether its export controlled data has been compromised in a cybersecurity incident or what the legal implications of the compromise might be under the export control laws. Identifying which critical data, networks, or services should be prioritised for the greatest protection is a key component of any risk-based cyber incident response plan. Controlled technical data resulting in export controls violations should be considered as part of this process.

The organisation should have a clear understanding of whether and to what extent the data it receives, transfers or stores constitutes export controlled technology, and the jurisdiction and classification of such data under the relevant regime(s). In cases of uncertainty, it should seek assistance in determining the export control jurisdiction and classification of its data. Moreover, knowing where such export controlled technical data is located can also be critical in identifying and assessing potential compromise of the company's export controlled information and the legal considerations relating to an appropriate response. In certain circumstances, placement of export controlled data (or certain highly restricted subsets of that data), on dedicated and easily identifiable servers may be an appropriate risk mitigation measure from both an export control and cybersecurity perspective.

Integrating export compliance stakeholders and procedures

Another key element of an effective incident response plan is the involvement of critical stakeholders, both in development and at the operational and response stages. Incident response teams should have an awareness and a clear understanding of how export controls apply to the company's technology and how that translates into incident response planning. To the extent the company has export control personnel, they should be involved early at the risk assessment and planning stage as well as being incorporated into the response team.

To the extent the company has both an export control program and IT/cybersecurity policies and procedures, the two should not exist in silos. The export control programme should include IT-based controls that are consistent with – and reinforce – the cybersecurity policies and procedures, and vice versa. It is also important that there be clear and mutually reinforcing lines of communication with respect to key stakeholders for both programmes.

Incident response: integration of export control considerations

Organisations with a thorough incident response plan will have a roadmap to act upon, including assessment of the nature, origin, and scope of the intrusion. It is important that incident response plans for companies with export controlled technology include legal coordination with respect to the potential regulatory requirements, including a determination of whether and to what extent any exfiltrated data was subject to export controls. If so, organisations should determine the relevant US government department or agency involved, the nature of any potential breaches, and whether or not there may be potential positive reporting obligations based on what is known about the facts and circumstances.

Tamer Soliman is global head of the Export Control & Sanctions practice at Mayer Brown, where David Simon is a partner in the Cybersecurity and Data Privacy practice, and Gretel Echarte Morales is an associate.

tsoliman@mayerbrown.com

dsimon@mayerbrown.com

gecharte@mayerbrown.com

This article is reprinted from the September 2017 issue of *WorldECR*, the journal of export controls and sanctions.
www.worldecr.com