ALISON NEWSTEAD, PARTNER,
SHOOK, HARDY & BACON INTERNATIONAL LLP

CYBER ALERT! MANUFACTURERS FACE SIGNIFICANT FINANCIAL PENALTIES FOR PRODUCT CYBERSECURITY FAILURES

Product safety issues affecting children quickly attract the attention of parents, regulators and the media. Toy manufacturers and suppliers are therefore acutely conscious of the importance of ensuring the safety of products prior to placing them on the market and throughout their lifecycle.

As toys have become more technologically advanced, the list of potential safety issues toy manufacturers must consider has expanded considerably. It is no longer sufficient to confine risk assessments to physical, mechanical, chemical, electrical, flammability and hygiene issues. New considerations – in particular cybersecurity – are now posing additional safety related risks and must be considered.

Just a few years ago, manufacturers, consumers and regulators would not have envisaged the need to recall a product like a smart watch or an interactive doll because of cybersecurity risks. Now the potential for recalls due to cybersecurity risks is very real.

Cybersecurity vulnerabilities are a threat to all products, including toys. As a result, the European Commission has proposed the Cyber Resilience Act (the CRA), the first ever EU-wide legislation on the cybersecurity of products.

In accordance with the CRA, manufacturers who place products on the market in the EU will need to give careful consideration to the cyber risks of products with digital elements, including toys. The CRA is likely to place a significant additional burden on toy manufacturers and those in the toy supply chain, with non-compliance attracting potentially weighty penalties.

What is the aim of the new Cyber Resilience Act?

The CRA introduces mandatory cybersecurity requirements for products with digital elements. The whole lifecycle of the product is considered, so obligations continue even when the product is in the hands of the consumer.

The aim of the CRA is twofold: to ensure that digital products are more secure, and to make sure consumers are better informed about the cybersecurity of the products they use.

Which products are covered?

The CRA applies to all products with a digital element which have a data connection to a device or a network. There is an exception for products that already have sector-specific legislation that deals with cyber issues, such as medical devices and cars.

It is of note that the European Commission's recent Consultation concerning the revision of the Toys Directive raised the issue of including new cybersecurity provisions. Consumers were very much in favour of including such amendments relating to protection of privacy, cybersecurity and psychological harm. Industry groups were less supportive of specific measures, perhaps as a result of the pending publication of the CRA.

With no current sector-specific provisions as to toy cyber-security in force, the provisions of the CRA will be applicable.

What will manufacturers and those in the supply chain need to do?

The CRA considers the entire lifecycle of products. Not only will toy manufacturers need to consider cybersecurity in the design, development and production of products, but they will also be expected to be transparent with customers about cybersecurity issues and ensure that there are security updates when needed. Any vulnerabilities which become apparent will also need to be handled effectively. This latter obligation will apply for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter.

Information and instructions must also be provided to consumers to ensure that toys with digital elements can be installed, operated and used securely. Prior to placing the toys on the market, a risk assessment will also need to be conducted. That evaluation will need to be updated when cyber vulnerabilities become evident through information received, whether through those in the supply chain, regulators or other third parties.

Who will be responsible for cybersecurity of toys?

In addition to manufacturers' obligations in the design and production phase, other economic operators in the supply chain, such as importers and distributors, will also have responsibilities.

How will the CRA be enforced?

Individual member states will carry out market surveillance and enforcement of the CRA in much the same way as general product safety issues are currently enforced.

Manufacturers and those in the supply chain will have a duty to notify the European Union Agency for Cybersecurity (ENISA) of any non-compliance within a very short timeframe: without undue delay and in any event within 24 hours of becoming aware of the non-compliance.

As with obligations under the Toys Directive, if a product is found not to be in compliance with the relevant cybersecurity requirements, steps must be taken to bring the product back into conformity or to withdraw or recall the product, as appropriate.

What are the potential penalties for non-compliance with the CRA?

Failure to comply with the requirements set out in the CRA can result in financial penalties. Economic operators who do not comply with the essential cybersecurity requirements may be subject to fines of up to EUR 15,000,000 or, if the offender is an undertaking, the fine may be up to 2.5% of its total worldwide annual turnover for the preceding financial year, whichever is higher. Non-compliance with any other obligations under the CRA will be subject to a fine of up to EUR 10,000,000 or, if the offender is an undertaking, up to 2% of its total worldwide annual turnover for the preceding financial year, whichever is higher. These are significant sums.

What should toy manufacturers and other stakeholders do?

Toy manufacturers and those in the toy supply chain who market products in the EU should expect to face far-reaching new requirements to ensure that those products are cybersecure.

Consulting the essential requirements in the proposed CRA now will give stakeholders an indication of their future obligations. Steps can be taken at this stage to make changes to processes and protocols to ensure compliance before the new Regulation comes into force.