Business Across Borders

Graham Bright, Compliance Director, Euro Exim Bank
(graham.bright@euroeximbank.com)

Nations are almost always better off when they buy and sell from one another. For businesses, globalisation can open up a world of opportunities. Access to the global economy provides new markets, new trade, new routes to consumers and new revenue streams, and nations with fundamental economic, social, political and cultural advantages.

Trade and cybersecurity are increasingly intertwined. Digital trade is crucial for almost every company, but it also introduces new complications. When products or services that contain a computer or can be connected to the internet - cross borders, cybersecurity risks emerge. And for today's CISOs, managing cyber risk is Job #1, and it's a full-time concern.

The role of trade finance is to introduce a third party to transactions to eliminate payment and supply risks. Businesses, organisations, and citizens increasingly operate online to deliver economic, social and other benefits. A recent McKinsey survey found that the pandemic has accelerated the overall adoption of digital technologies and applications by three to seven years in just a few months.

At the same time, cybersecurity threats have been growing. Large-scale fraud, data breaches, and identity thefts are increasing. The *World Economic Forum's Global Cybersecurity Outlook* report indicates that cyber-attacks increased 125% globally in 2021, with evidence suggesting a continued uptick through 2022.

There are many financial institutions focusing on international trade, and *Euro Exim Bank (EEB)* is the one to watch. Unlike a retail bank with counters, current accounts and holding client cash, *EEB* uses online 3rd party accounts with global banking counterparts and is constantly vigilant against cyber-attacks.

Government Capability in Managing Cybersecurity Risks:
According to the OECD, cybersecurity should *"aim to reduce the risk to an acceptable level relative to the economic and social benefits expected from those activities, while taking into account the legitimate interests of others."*

We are highly dependent on electronic technology in the modern world, and protecting this data from cyber-attacks is a challenging issue. A government's reactions are shaped by its capability to manage cybersecurity risks, such as: the laws and regulations on cybersecurity; the implementation of technical capabilities through national and sector-specific agencies; the organizations implementing cybersecurity; and the awareness campaigns, training, educations, and partnerships between agencies, firms, and countries.

The low cost of entry, anonymity, uncertainty of the threatening geographical area, dramatic impact and lack of public transparency, have led to strong and weak actors including governments, organized and terrorist groups and even individuals in this space, and threats such as cyber warfare, cybercrime, cyber terrorism, and cyber espionage. Governments must devise efficient systems to protect against the destructive impacts of cyber threats.

Many governments are introducing new policies to help increase their cyber security. The UK government for example has published the *Government Cyber Security Strategy (2022-2030)* in which is sets out the government's approach to building a cyber resilient public sector.

What is cybersecurity compliance?
Cybersecurity compliance is the organizational risk management method aligned with pre-defined security measures & controls on how data confidentiality is ensured by its administrational procedures. IT security is made more challenging by compliance regulations, such as HIPAA, PCI DSS, Sarbanes-Oxley and global standards, such as GDPR.

Cybersecurity standards:
Cybersecurity standards represent a key step in the IT governance process. As a means for managing and containing risk to acceptable levels, the standards must be wholly consistent with IT governance instruments and closely aligned with and driven by the enterprise's cybersecurity policies. Standards can build a common approach to addressing cybersecurity risks based on best practice.

The International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) have developed a number of cybersecurity-related standards, including the jointly developed ISO/IEC 27000 series as well as sector specific-standards for electric utilities, healthcare, and shipping.

To address global cybersecurity challenges and improve digital trust, a new and improved version of ISO/IEC 27001 has just been published. The world's best-known standard on information security management helps organizations secure their information assets – vital in today's increasingly digital world.

Certification of compliance with cybersecurity standards:
Compliance certification can give business confidence in the cybersecurity of organizations and government. Under the *EU Cybersecurity Act*, June 2019, the *European Union Agency for Cybersecurity* will establish an EU-wide cybersecurity certification scheme. NIST has developed a different approach in the Baldridge Performance Excellence Program, which encourages self-assessment of compliance.

Using Trade Policy to Improve Cybersecurity:
Although digital trade increases cybersecurity risks, trade and cybersecurity policy can also work in tandem to support growth in digital trade as well as strengthen cybersecurity outcomes.

Reforms since World War II have substantially reduced government-imposed trade barriers. But policies to protect domestic industries vary. Tariffs are much higher in certain sectors and among certain country groups than in others. Many countries have substantial barriers to trade in services in areas such as transportation, communications, and, often, the financial sector, while others have policies that welcome foreign competition. Under the rules-based international trading system centred in the WTO, trade policies have become more stable, more transparent, and more open.

Access to data:
As cybersecurity defence becomes more sophisticated, use of analytics and machine learning to monitor network activity plays a growing role in the analysis of risks and anomalies. The CPTPP and USMCA commitments to information flows across borders (subject to appropriate exceptions) and to avoiding data localization requirements, advances digital trade opportunities and cybersecurity outcomes.

Information sharing:
Trade agreements can include commitments to building public and private sector information sharing mechanisms. For example, the U.S.-Mexico-Canada trade agreement includes a commitment to sharing information and best practices as a means of addressing and responding to cyberattacks.

Why a risk-based approach to cybersecurity is the right business choice:
Monitoring of trade deals needs a risk-based approach. The move from a free trade approach to a risk-based approach marks a foundational shift thinking on trade. This has prompted an urgent development of new policies, which includes a greater reliance on export controls. Cybersecurity is one of the main topics for business managers in today's world. The approach to cyber risks has changed from "maturity based" to "risk-based" over time.

Risk-based approaches are often presented in opposition to compliance-driven approaches. A risk-based approach to cybersecurity is also proactive rather than reactive. Instead of focusing on incident response, a CIO at an organization using this approach is likely to invest heavily in testing, threat intelligence, and prevention. Finally, this approach is inherently realistic. The goal of a risk-based cybersecurity program is meaningful risk reduction, not 100% security.

New trade rules that can both support risk based effective cybersecurity regulation, build bridges between the cybersecurity policy in different countries to maximize synergies, and minimize barriers to trade are needed.

Euro Exim Bank (EEB) complies with the ever-changing policies and is a global organisation that caters to many countries with different jurisdictions, enacting end-to-end security and frequent evaluations with ongoing improvements. EEB was an early participant in the Ripple community and achieved xCurrent connectivity enabling institutions to instantly communicate and settle cross-border payments with end-to-end visibility and tracking, all in record time. EEB also participates with Ripple's ODL service, and with expansion of crypto globally, looking to issue its own stable coin in 2023.

As the digital economy is growing, so too is the opportunity for malicious actors to exploit IT vulnerabilities. Recent high-profile cyber incidents, such as *SolarWinds* and *Microsoft Exchange*, along with the notable increase in ransomware attacks on organisations and critical national infrastructure such as the Colonial Pipeline in the US, have demonstrated the disruptive potential of these threats and the real world impacts they can bring about.

Doing nothing is no longer an option. You can protect your organisation, and your reputation, by partnering with a well-recognized financial organisation like EEB, with years of experience for effective management of risk in the facilitation of global trade.