Bruno Castro
Fundador & CEO da VisionWare
Especialista em Cibersegurança e Investigação Forense
Founder & CEO of VisionWare, Cybersecurity and Digital Forensics Specialist

A CIBERSEGURANÇA COMO CONDIÇÃO PARA EXPORTAR COM SUCESSO

Cybersecurity as a condition for successful exporting

As exportações estão cada vez mais digitais, e mesmo quando o produto final é "físico", a realidade é que todo o processo em redor da venda depende de sistemas informáticos: plataformas de logística, softwares de gestão, serviços de marketing digital, pagamentos eletrónicos, ferramentas de comunicação, armazenamento de dados de clientes, etc. E é precisamente nesse ecossistema digital que a cibersegurança se tornou um fator crítico para quem "vende para fora".

Durante muitos anos, a segurança digital foi vista como um problema interno: proteger servidores, controlar acessos, evitar a entrada de vírus, garantir a estabilidade da infraestrutura. Mas a economia digital mudou essa lógica, e hoje, qualquer empresa exportadora está inevitavelmente ligada a dezenas de plataformas e fornecedores externos, desde agências de marketing, serviços cloud, operadores logísticos, plataformas de e-commerce, ferramentas de CRM, gateways de pagamento, entre muitos outros. Existe um constante cruzar de ecossistemas digitais com maturidades e obrigações completamente distintas no que respeita a cibersegurança.

O caso da Mango no ano passado ilustra bem esta realidade. A empresa sofreu um ciberataque que teve origem num serviço externo de marketing utilizado para envio massivo de campanhas publicitárias. Houve acesso não autorizado a dados pessoais de clientes da Mango, embora, felizmente, informações sensíveis como dados bancários, credenciais ou documentos de identidade não tenham sido, aparentemente, comprometidos. Ainda assim, o episódio mostra uma verdade que as organizações já não podem ignorar: o risco já não está apenas dentro da empresa.

Para empresas exportadoras, este ponto é muito sensível, e quando se opera em mercados internacionais, os fluxos de dados multiplicam-se em várias dimensões cibernéticas. Na prática, cada parceiro tecnológico torna-se uma extensão do perímetro digital de cada empresa. É precisamente neste contexto que a diretiva NIS2 ganha maior relevância ao vir reforçar, de forma significativa, as obrigações de cibersegurança e, sobretudo, colocar um foco claro na gestão de risco na cadeia de fornecimento. A mensagem é simples: não basta apenas proteger os sistemas internos, é necessário garantir que os parceiros externos mantêm níveis adequados de segurança para poderem conviver comigo neste ecossistema digital sem colocar em causa a nossa segurança, e por inerência, a viabilidade do próprio ecossistema e da sua atividade comercial.

Para empresas que exportam, tal significa uma mudança de abordagem. A escolha de fornecedores tecnológicos passa a exigir um grau de escrutínio que, até há poucos anos, era raro. Não basta avaliar preço, funcionalidade ou rapidez de implementação. É necessário questionar práticas de segurança, certificações, processos de gestão de incidentes e políticas de proteção de dados para que a inclusão dos parceiros de negócio não venha colocar em causa o risco interno de todos os que convivem nesse ecossistema. A inclusão de um parceiro imaturo em termos cibernéticos irá, mais cedo ou mais tarde, colocar em causa os restantes elementos do ecossistema.

Na prática, isso pode traduzir-se em várias medidas algo simples, mas muitas vezes negligenciadas: incluir cláusulas de segurança em contratos com fornecedores, exigir evidências de certificações ou auditorias independentes, avaliar regularmente o risco associado a serviços externos, e definir procedimentos claros para a resposta a incidentes que envolvam terceiros.

A lógica é semelhante à gestão de qualidade na cadeia de fornecimento física. Tal como uma empresa exportadora se preocupa com a qualidade dos componentes ou matérias-primas, deve também preocupar-se com o nível de maturidade da sua segurança digital e dos serviços tecnológicos que utiliza. Porque, no final, o impacto reputacional de um incidente recai sempre sobre a marca principal. A cibersegurança está a tornar-se um novo fator de competitividade no comércio internacional e na economia digital, e a (ciber)segurança também viaja com a marca.

Companies must examine security practices, certifications, incident management processes and data protection policies to ensure that the inclusion of business partners does not expose the entire ecosystem to internal risk. The inclusion of a partner with immature cybersecurity practices will, sooner or later, put the rest of the ecosystem at risk.

É necessário questionar práticas de segurança, certificações, processos de gestão de incidentes e políticas de proteção de dados para que a inclusão dos parceiros de negócio não venha colocar em causa o risco interno de todos os que convivem nesse ecossistema. A inclusão de um parceiro imaturo em termos cibernéticos irá, mais cedo ou mais tarde, colocar em causa os restantes elementos do ecossistema.

Exports are becoming increasingly digital, and even when the final product is "physical", the reality is that the entire process surrounding the sale depends on IT systems: logistics platforms, management software, digital marketing services, electronic payments, communication tools, customer data storage, and so on. It is precisely within this digital ecosystem that cybersecurity has become a critical factor for companies that sell internationally.

For many years, digital security was seen as an internal issue: protecting servers, controlling access, preventing viruses from entering systems and ensuring infrastructure stability. But the digital economy has changed that logic. Today, any exporting company is inevitably connected to dozens of external platforms and providers, from marketing agencies and cloud services to logistics operators, e-commerce platforms, CRM tools and payment gateways, among many others. There is a constant intersection of digital ecosystems with completely different levels of maturity and obligations when it comes to cybersecurity.

Last year's case involving Mango illustrates this reality well. The company suffered a cyberattack originating from an external marketing service used to send large-scale advertising campaigns. There was unauthorised access to Mango customers' personal data, although fortunately sensitive information such as banking details, credentials or identity documents does not appear to have been compromised. Even so, the episode highlights a reality that organisations can no longer ignore: risk no longer resides solely within the company.

For exporting companies, this issue is particularly sensitive. When operating in international markets, data flows multiply across multiple cyber dimensions. In practice, every technology partner becomes an extension of the company's digital perimeter. It is precisely in this context that the NIS2 directive gains greater relevance, significantly strengthening cybersecurity obligations and, above all, placing a clear focus on supply chain risk management. The message is simple: it is not enough to protect internal systems. Companies must also ensure that external partners maintain adequate security standards so they can operate within the same digital ecosystem without compromising the security — and ultimately the viability — of that ecosystem and its commercial activity.

For exporting companies, this implies a shift in approach. The selection of technology suppliers now requires a level of scrutiny that was rare until a few years ago. It is no longer enough to assess price, functionality or speed of implementation. Companies must examine security practices, certifications, incident management processes and data protection policies to ensure that the inclusion of business partners does not expose the entire ecosystem to internal risk. The inclusion of a partner with immature cybersecurity practices will, sooner or later, put the rest of the ecosystem at risk.

In practice, this may involve several relatively simple but often overlooked measures: including security clauses in supplier contracts, requiring evidence of certifications or independent audits, regularly assessing the risk associated with external services and defining clear procedures for responding to incidents involving third parties.

The logic is similar to quality management in a physical supply chain. Just as an exporting company is concerned about the quality of its components or raw materials, it must also pay attention to the maturity of its digital security and the technological services it relies on. In the end, the reputational impact of any incident always falls on the main brand. Cybersecurity is becoming a new factor of competitiveness in international trade and in the digital economy — and (cyber)security travels with the brand.