Expert Group

Secure E-Commerce

Supply-Chain Security in Digital Commerce

shopping tomorrow

Takeaways

1. Unlike other industries, the retail sector lacks an umbrella organization for the exchange of information about cyber-threats.
2. The information exchanged on this subject on this subject must be appropriate to individual organizations' level of cybermaturity and must be timely and relevant.
3. Legislators support appropriate technical standards being applied regarding data exchange between systems, including email.

Host

Chair

Supply-Chain Security in Digital Commerce

The popularity of online consumer shopping continues to rise. Due to the significant increase in the use of online channels, we are seeing a growing shift of fraud and insecurity from the domain of traditional, physical retail to digital commerce. Data is shared at various stages of the supply chain (from purchase right through to delivery), giving rise to any number of vulnerabilities. There are numerous security-related issues affecting e-commerce. Our research focused on two issues arising in the supply chain, with the purpose of presenting supply-chain partners with a number of priorities and checklists that can help to strengthen the supply chain and reduce its vulnerability. We decided to focus on medium-sized to large companies. The first chapter addresses data exchange (including online data exchange) in the supply chain, so as to ensure that businesses are more aware of current threats, and can anticipate these threats and take the appropriate precautions. The second chapter describes a different form of data sharing, namely the exchange of technical data between the various systems across the e-commerce supply chain.

1. Cyber Information Exchange in the Supply Chain

In a report commissioned by the Dutch Cyber Security Council titled De economische en maatschappelijke noodzaak voor meer Cyber Security: Nederland Digitaal Droge Voeten ("Keeping Our Digital Feet Dry: The Economic and Societal Necessity of Improved Cyber Security"), PostNL CEO Herna Verhagen urges businesses to share information on cybersecurity.[1] [2]The Cyber Security Council also concludes, in its second advisory report for 2017, that current efforts to educate organizations about cybersecurity are focused mainly on the Dutch national government and organizations within the vital infrastructure. Any businesses that have not been classified as 'vital infrastructure' have not, to date, received any information from the government regarding vulnerabilities and threats, which means they have an information deficit, whether they are aware of it or not. In addition, businesses tend to have no link to any other kind of network or pre-existing structures for the sharing of cybersecurity-related information – or are failing to exchange this kind of information in a systematic manner. Specifically, there is currently no nationwide network of information hubs in place to assist and support businesses in this area.

This study focuses on information sharing between medium-sized and large e-commerce companies with annual revenue exceeding €300,000. Within this group, we distinguish between three levels of experience as far as information sharing is concerned. Each of these levels comes with its specific questions regarding the type of information and the appropriate approach:

1 VERHAGEN, 2016 (NEDERLAND DIGITAAL DROGE VOETEN (WWW.CYBERSECURITYRAAD.NL/BINARIES/CYBERSECURITYADVIESHERNAVERHAGEN_TCM56-122110.PDF))

2 CYBER SECURITY COUNCIL – ADVISORY REPORT #2 (WWW.CYBERSECURITYRAAD.NL/BINARIES/CSR_ADVIES_INFORMATIEUITWISSELING_NED_TCM107-314535.PDF)

1. **Basic:** I would like to start an information-sharing community. Where should I begin? Dos and don'ts.
2. **Advanced:** I already routinely exchange information. What can I learn in order to improve?
3. **Expert:** I have already been sharing cybersecurity-related information for quite some time. How can I change the information-sharing community in order to make the information-sharing process even more efficient and effective?

Businesses don't just start sharing information with each other unprompted, particularly if the information concerned is considered sensitive. There must be positive incentives encouraging them to start doing so. This has been the subject of a study by the European Union Agency for Network and Information Security (ENISA). Various interviews revealed that cost savings are a key incentive for initiating (and/or increasing the level and frequency of) information sharing, while[3] the quality, value, timeliness, and use of the shared information also play a crucial role.

What type of information on cybersecurity organizations need depends heavily on their level of *cybermaturity* . Companies that are not mature, or have a lower level of cybermaturity, tend to have a need for more generic information, such as guidelines, best practices, and action plans. Companies that are cybermature, for their part, have a need for high-quality information regarding threats and vulnerabilities. While a company's level of cybermaturity tends to be related to its size, this is not always the case. Information sharing (whether by the government or between companies) must be appropriate for the target audience.

1.1 What Are the Various Types of Information Sharing?

Sharing sensitive data and information is a complex subject. The sharing of information about incidents and vulnerabilities affects organizations at the strategic, tactical, operational, and technical levels and comprises all stages of the *cyber incident response*cycle (i.e. prevention, preparation, incident response, recovery, and aftercare/follow-up.) As such, it transcends the boundary between the public and private domain and comes with an inherent quandary: much of this data is sensitive and can therefore potentially be harmful to the organization, while it can be highly useful and practical to others at the same time.[4]

ISACs (*Information Sharing and Analysis Center*s) have been created for companies operating within the vital infrastructure, including energy providers and telecommunications companies, to share cybersecurity-related information. There are already a number of initiatives in place or underway for other sections of the corporate sector; a non-exhaustive list is included in the table on the next page. However, these information hubs do not constitute a comprehensive nationwide system for all companies – for example, there is no sector-wide information hub for the e-commerce supply chain.

3 LUIJF & KERNKAMPF, 2015, SHARING CYBER SECURITY INFORMATION (WWW.PUBLICATIONS.TNO.NL/PUBLICATION/34616508/OLYFG9/LUIIJF-2015-SHARING.PDF)

4 HUISTRA & KRABBENDAM-HERSMAN, 2017, TNO VERKENNING CYBERSECURITY INFORMATIEDELING BINNEN DE TOPSECTOREN ("ANALYSIS BY THE NETHERLANDS ORGANIZATION FOR APPLIED SCIENTIFIC RESEARCH OF CYBERSECURITY INFORMATION SHARING WITHIN THE KEY SECTORS"), (WWW.RIJKSOVERHEID.NL/BINARIES/RIJKSOVERHEID/DOCUMENTEN/RAPPORTEN/2017/03/07/VERKENNING-CYBERSECURITY-INFORMATIEDELING-BINNEN-DE-TOPSECTOREN/CYBERSECURITY+INFORMATIEDELING+BINNEN+DE+TOPSECTOREN.PDF)

Vital companies and sectors	Non-vital companies and sectors
ISACs	• Non-vital ISAC (examples: the Legal-ISAC and Connect2Trust) • Digital Trust Center (affiliated with the National Cyber Security Center, but does not focus exclusively on critical infrastructure) and various related initiatives devoted to knowledge-sharing and awareness, the DTC website and (in 2019) the DTC Platform, along with other websites such as alertonline.nl and veiliginternetten.nl;
• Sectoral and regional initiatives, including Brainport, Z-CERT, the Cybersecurity Center for the Manufacturing Industry, FERM, CYSSEC, and NIDV Cyber-Resilience.	

List of organizations and structures for sharing cybersecurity information

The initiatives listed in the table receive (or will receive) information directly from the government regarding threats and the options available for taking action. This is, in fact, enshrined in a new law in the Netherlands known as the Network and Information Systems Security Act, which entered into force on November 9, 2018. In order to be eligible to receive information directly from the Dutch government, initiatives must fall into one of the following three categories:

- Organizations whose demonstrable, objective duty it is to inform other organizations or the public on these issues. This category includes, for example, the ISACs and Brainport.
- *Computer Security Incident Response Teams* (CSIRTs). These include, for example, the Z-CERT emergency response team that was created for the healthcare sector.
- Other computer crisis teams, as designated in the regulations issued by the Ministry of Justice & Security or falling within a category designated under these regulations.

1.2 What Information-Sharing Channels Are Available?

Information-sharing channels in the Netherlands tend to be affiliated with the previously listed initiatives and incentives. These can be consolidated into the following three types of information sharing:

1. **One-on-one information sharing:** In this situation, information is shared between only two – or among a select number of – companies. Digital resources may be used for this purpose, including secure environments, encrypted email, and face-to-face conversations, e.g., in the context of, or in addition to, an ISAC.
2. **One-on-N information sharing:** In this situation, information from a single entity is shared with as many parties as possible. Examples of this include sharing information through websites (digitaltrustcenter.nl and security.nl) or through an app (CyberAlerts), with the sender (the 'one') addressing as many recipients (the 'N') as possible. Another example of one-on-N information sharing is a company requesting support from a larger pool of players – for example within a specific sector – rather than asking for one-on-one support. These queries tend to be related to the impact of, for example, new legislation (such as the GDPR) or the implementation of new technologies.
3. **N-on-N information sharing:** This scenario involves the creation of online platforms where entire groups exchange information with each other. In 2019, the Digital Trust Center will be launching a new service called the Digital Trust Platform for this purpose, but communities on social media (including on WhatsApp and Facebook) and various platforms launched by industry associations are also examples of venues for N-on-N information sharing.

1.3 Conclusions and Recommendations for E-Commerce Companies

Major Dutch e-commerce organizations such as PostNL and Jumbo – which maintain extensive networks of partners and suppliers – understand how important it is to provide the organization with the right information at the right time regarding cyber threats and potential actions to be taken by attackers. After all, the timely provision of information makes it possible, for example, to take preventive measures, thereby mitigating the impact of an attack, or to take corrective measures in the event of an incident as efficiently and effectively as possible. These efforts are aimed at reducing the impact on the business processes and objectives to a minimum – in other words, ensuring that regular business can continue without interruption.

In view of the complex environment and the large variety of supply-chain partners, we again underscore the importance of exchanging information regarding cyber threats and potential measures to be taken. In addition to the economic incentive, it is in the public interest for major e-commerce companies to participate in various initiatives to facilitate or promote information exchange.

Our research has shown that, while there are various forums, task forces, and platforms for sharing information on threats, there is no specific platform for businesses operating in the e-commerce supply chain where information is shared on cyber threats and potential measures to be implemented. This means that these companies are not provided with the latest information on threats relating to existing and new attack vectors that actually constitute a threat to the e-commerce supply chain.

The establishment of an e-commerce ISAC, which already exists in the United States (**r-cisc.org**) could be valuable in this regard, particularly for large e-commerce organizations. These sectoral ISACs make it possible to share information in a secure, familiar environment relating to incidents, vulnerabilities, and threats to the sector and the supply chain. In addition, it is useful to share information across different sectors and industries.

At the same time, our study revealed that companies may have differing reasons for wanting to get involved with information sharing. Smaller companies have different types of information needs and a different scope for action than large e-commerce companies that can get their information from ISACs. The process of analyzing and correlating data, for example, requires a level of expertise that many companies simply do not have. Medium-sized and smaller e-commerce companies need to be provided with information appropriate to their specific situation through some other method or channel.

Experience has shown that industry associations can play a key role in this, as they keep records on – and enjoy a position of trust among – their members. This is also why we believe Thuiswinkel.org has a key role to play as an information hub for members of all sizes. We therefore recommend that Thuiswinkel.org create a designated space within the DTC platform with information for the retail sector. Thuiswinkel.org might be able to gain inspiration from similar joint initiatives already in place, including Brainport, FERM, and CYSSEC, as well as from cyber-resilience projects initiated in the southern Dutch province of Limburg and the northern Netherlands. We believe that large cybermature e-commerce companies also have a role to play within the industry; they could, for example, offer seminars on the subject of cybersecurity.

2. Secure Interfacing in the E-Commerce Supply Chain

In the previous chapter, we explored opportunities for the exchange of cyber information between the various players in the e-commerce supply chain. In this chapter, we will discuss the exchange of technical data between the various systems in the supply chain and how this can take place securely.

It is important for businesses to establish a clear set of security standards. As with many other business risks, prevention is the best cure. Achieving the appropriate level of security involves more than simply maintaining your organization's reputation and avoiding damage caused by digital attacks: it also includes compliance with the relevant laws and regulations. Organizations tend to outsource many of the activities related to data protection and the management of network and information systems. However, the company itself remains liable for correctly processing the data, which means data breaches and the abuse of data and systems remain a business risk. Making agreements with – and supervising – providers of specialized services ensures that payment processing, data storage, and the protection of any business secrets take place in a way that is reliable and covers all bases.

2.1 Checklist for Partners, Buyers, and Suppliers

Increasingly, essential parts of companies' business operations are delivered outside the organization's physical environment. Web applications and data storage through cloud providers are both examples of this. In order to provide you and your business with the appropriate support, we joined forces with various e-commerce and security experts to draw up a checklist. The purpose of this checklist is to enable you to learn more about the security of your business data and processes when these are shared with third parties through interfacing. Ask your partners, customers, and suppliers to complete the checklist, following which you can determine which points are relevant to you.

Paragraphs 2.2 to 2.4 provide background information on the checklist, while the checklist itself can be found in paragraph 2.5.

2.2 Data Storage

E-commerce companies tend to store large amounts of data relating to their customers, customer orders, and payments, along with information on partnerships, employees, and suppliers, such as purchasing and salary information. This sensitive information is not supposed to be accessible to third parties. Examples of effective security measures include:

- Restricting access to information to a select group of users.
- Keeping a log of who accessed what data and when.
- Encrypting data before storing it in a file or database.
- Making sure that some types of sensitive data, including payment details and medical records, are not stored, or are deleted automatically once the service has been provided.

When sending data relating to your business or customers to suppliers or third parties, you can ask about the security measures implemented by these parties.

2.3 Changing Laws and Regulations

Protecting information systems comes with its share of obligations. Just as office buildings have fire safety regulations in place, there are specific requirements for data processing to comply with security levels imposed by the applicable laws and regulations. We want to emphasize here that it is the data owner who is liable, rather than the party providing the data-management or data-processing services. This means that infringements by third parties could also result in fines or reputational damage.

Two aspects that play a role here are entrepreneurship and risk assessment. The overall thrust of the legislation regarding[5] personal data is as follows: *The data controller must implement the appropriate technical and organizational measures for protecting data (including personal data), taking into account the state of the art, implementation costs, and the level of risk involved.* There are no specific requirements such as: "Everyone must have an antivirus product installed on all of their systems." The legislative framework for data security is based on the premise that organizations can set priorities independently according to the "comply or explain" principle, with the decision of whether or not to implement a certain measure being based on an in-depth risk analysis.

A calculated risk might be to allow employees to use business computers, laptops, and mobile devices for personal purposes in order to facilitate the New World of Work, provided that they agree to comply with an "acceptable use" guideline, which specifies what types of usage are and are not authorized. While awareness campaigns and training courses are sometimes considered superfluous, they do help employees realize how easy it is to get access to information and what the consequences can be. Scheduling regular training sessions – possibly with an attendance requirement – and sharing best practices will help you improve your security culture.

2.4 Secure Communication Between Your Company and Its Suppliers

There are various ways in which businesses can exchange information and data with suppliers. Some suppliers might provide a standard portal or API-style solution, while others simply use email as a means of communication.

In any event, it is important to facilitate secure communications between your business and its suppliers. In other words, anyone with malicious intent who is able to intercept communications being transmitted should not be able to view the data being communicated. In the next few paragraphs, we will discuss some of the most common interface options and specify the issues associated with each of these options.

API or Web Service

The supplier's API or web service can be used to transmit data. The majority of APIs are based on SOAP (which uses XML messages) or REST (which tends to use XML or JSON messages). The supplier generally provides a user account that allows you to authenticate with the web service.

In order to prevent attackers from accessing your communications, it is essential to use a secure (SSL/TLS) connection. With web-based APIs, you can recognize a secure connection by the https:// prefix in the address bar (instead of http://).

FTP, SMB, and Other File-Sharing Services

You can upload and download files directly by logging onto a file-sharing service provided by your supplier. A user account is usually required to establish a connection.

5 WWW.PRIVACY-REGULATION.EU/NL/ARTIKEL-32-BEVEILIGING-VAN-DE-VERWERKING-EU-AVG.HTM

Some of these file-sharing services do not normally use secure connections. Services such as SFTP, FTPS, and SSH, however, do use secure, encrypted connections.

If the service works with a website you can access through your browser or a mobile app, make sure the URL starts with "https" and that you see a padlock icon in the address bar.

It is often not necessary to make a file-sharing service accessible across the entire internet; the technology is available to restrict access to the service to, for example, a number of specific IP addresses, which reduces the risk of system attacks.

Email

If you use email to share data with your suppliers, you should be aware that email is an inherently insecure medium. For one, most email providers do not use a secure connection to send and receive messages. It is also relatively easy to send emails in the name of another person or another domain.

There are a number of technical and organizational measures you can take to be able to use email securely despite these inherent risks. At the organizational level, you can, for example, train employees to spot fake emails. This reduces the risk of employees unintentionally downloading malicious software (malware) or sharing data with people with malicious intentions (phishing).

In addition, it is possible to implement a number of technical measures to improve the security of sending and receiving email. Check that your email system uses the appropriate email standards, e.g., DMARC, DKIM, SPF, and TLS/STARTTLS. There are several sites where you can verify this, including**www.internet.nl.** Show your system administrator the test results and ask them to implement the appropriate standards.

2.5 Checklist

With the background information from the previous paragraphs in mind, you can use the checklist below to survey your partners, customers, and suppliers, and make them aware and remind them of their responsibilities if necessary.

Data Storage, Laws, and Regulations

You are sharing data regarding your business and/or customers with a third party:

- Is data relating to my business and/or my customers stored separately from data relating to other customers?
- Is encryption used to store data relating to my business and/or my customers?
- How long is data relating to my business and/or customers retained?
- How is data relating to my business and/or customers used by the supplier?
- Is the organization's approach to the storage of personal data GDPR-compliant?
- Do they comply with any other privacy-related and security-related guidelines?
- Do they regularly install the latest software patches and updates on their systems?

You use data-processing systems yourself:

- Are regular vulnerability scans performed on systems that are directly accessible over the internet?
- Is employee awareness being raised through, for example, awareness training?
- Does the business use monitoring solutions that, for example, store access logs in one central location and make these searchable?

Secure Communications Between Your Company and Its Suppliers

You are using an API or web-service link with a third party:

- Is a user account or API key required to use the API? If so, does the account come with a password or key consisting of a minimum of 12 characters?
- Is a secure connection used for all communications (SSL/TLS)?

You are using a file-sharing service provided by a third party, e.g., FTP, SMB, or SSH:

- Is a user account required for the use of the file-sharing service? If so, does the account come with a password consisting of a minimum of 12 characters?
- Is a secure connection used (SSL/TLS)? Since SFTP, FTPS, and SSH services work with a secure connection as a rule, it is recommended that you use one of these services.
- Is the file-sharing service subject to restricted access?

You are using a customer, vendor, or cloud portal provided by a third party:

- Is a user account required for the use of the file-sharing service? If so, does the account come with a password consisting of a minimum of 12 characters?
- Is a secure connection used (SSL/TLS)?

You primarily use email to transmit data to another party:

- Does your business use a secure (SSL/TLS) connection for transmitting and retrieving email messages?
- Do your email systems provide sufficient protection against phishing?

HOSTS

Gerrie de Jonge
CIO, Parcels & Logistics
PostNLPakketten Benelux BV

Gunther Cleijn
Cybersecurity Officer
PostNL Pakketten Benelux BV

CHAIR

Roland van Kortenhof
Operations Manager
Thuiswinkel.org

Expert group members

Dennis Pieterse
Senior Security Advisor
T-Systems Nederland B.V.

Diederik Perk
Threat Intelligence Advisor
Fox-IT

Hans Minten
Master Security Analyst
wehkamp

Michel Teuwen
Senior Information Security Consultant
Jumbo Groep Holding B.V.

Nick Pinto
Fraud Team Leader
wehkamp

Nicole Mallens
Senior Policy Secretary
VNO-NCW & MKB-Nederland

Thomas Stols
Cybersecurity Specialist
Computest

Raymond van den Hoek
IT Security Manager
bol.com

Other contributors to this Blue Paper:

Raymond Bierens
PhD Researcher
Delft University of Technology