Elektrotechnik & Informationstechnik (2015) 132/2: 106–112. DOI 10.1007/s00502-015-0289-2

Cyber security information exchange to gain insight into the effects of cyber threats and incidents

F. Fransen, A. Smulders, R. Kerkdijk

The last couple of years we have seen an increase in interests and initiatives in establishing threat intelligence sharing communities, and on the development of standards and platforms for automated cyber security information sharing. These initiatives are focused on helping organisations to increase their resilience to new attacks and threats.

In this paper we will investigate how we can leverage from cyber security information sharing infrastructures to gain early insight into the large scale effects of cyber threats and incidents. In particular we focus on those that might have a disruptive effect on society. Furthermore, in this paper we will discuss what information needs to be shared and how this can be done using the dominant threat intelligence sharing standards.

Keywords: cyber security information sharing; threat intelligence; STIX—Structured Threat Information eXpression

Cyber Security-Informationsaustausch zur Erkennung von Cyber-Bedrohungen und -Vorfällen.

In den letzten paar Jahren erlebten wir einen Anstieg des Interesses als auch den Aufbau von Initiativen für den Austausch von Informationen über Cyber-Bedrohung zwischen Organisationen und für die Entwicklung von Standards und Plattformen für den automatischen Austausch von Cyber Security-Informationen. Diese Initiativen zielen darauf ab, Organisationen bei der Erhöhung ihrer Widerstandsfähigkeit gegen neue Attacken und Bedrohungen zu unterstützen.

In diesem Beitrag erörtern die Autoren, wie eine Infrastruktur zum Cyber Security-Informationsaustausch zu einem frühen Einblick in die großflächigen Effekte der Cyber-Bedrohungen und -Vorfälle verhilft. Im Besonderen sind jene Bedrohungsszenarien im Fokus, welche einen nachhaltigen negativen Effekt auf die Gesellschaft ausüben. Darüber hinaus wird in diesem Beitrag diskutiert, welche Information ausgetauscht werden muss und wie dies unter Einsatz der vorhandenen Standards in diesem Bereich geschehen kann.

Schlüsselwörter: Cyber Security-Informationsaustausch; Informationen über Cyber-Bedrohung; STIX—Structured Threat Information eXpression

Received January 7, 2015, accepted January 26, 2015, published online February 7, 2015

1. Introduction

The landscape of cyber threats is rapidly evolving. New vulnerabilities emerge at a tremendous pace and these vulnerabilities are increasingly qualified as severe. What's more, cyber-attacks are continuously becoming more sophisticated. State of the art malware is greatly autonomous and employs specific stealth techniques to avoid detection. High end targeted attacks are persistent and involve elaborate combinations of methods and attack vectors, ranging from specific technical exploits to social engineering of critical staff. On top of all this, attackers are increasingly organised by actively collaborating, sharing tools and techniques and offering services to one another.

In the midst of these developments, the dependency on ICT and thus the potential impact of any security incident is still going forward. Due to the dynamics in present day cyber threats, organisations cannot passively rely on traditional (preventive) measures. To avoid damages and disruptions, they must continually stay on top of the latest threats, vulnerabilities, attack methods and attacker campaigns. To this end, organisations are in need of appropriate threat intelligence.

Already a great variety of sources to acquire threat intelligence exist. We distinguish the following categories: company internal sources (e.g. from an IDS or SIEM), public sources (e.g. CERT advisories, threat reports), and commercial sources (e.g. Mandiant Intelligence Center). An upcoming and most promising source of threat intelligence are threat intelligence communities, i.e. networks of organisations, that start exchanging threat intelligence amongst each other. To speed up the intelligence sharing a need is growing for structured automated exchange of information. This is reflected in the recent increase in development of standards for threat intelligence sharing (e.g. CybOX, STIX and TAXII) and the development of platforms to support automated cyber security information sharing (e.g. MISP, Soltra Edge).

An example of the establishment of a recent threat intelligence community is the National Detection Network (NDN) from the National Cyber Security Center (NCSC) in The Netherlands. The NDN is a collaboration between NCSC, Dutch government organisations and critical infrastructure organisations, to share threat information in a better and faster way. NDN will enable the connected parties

Fransen, Frank, TNO, Eemsgolaan 3, 9727 DW, Groningen, The Netherlands (E-mail: frank.fransen@tno.nl); **Smulders, Andre,** TNO, Brassersplein 2, 2612 CT Delft, The Netherlands (E-mail: andre.smulders@tno.nl); **Kerkdijk, Richard,** TNO, Eemsgolaan 3, 9727 DW, Groningen, The Netherlands (E-mail: richard.kerkdijk@tno.nl)

to take appropriate measures to prevent and/or reduce damage, thereby increasing cyber resilience.

Threat intelligence is not only vital for ICT-intensive organisations seeking to maintain a solid level of cyber resilience, but also for bodies coordinating cyber security on a national level such as the NCSC in The Netherlands. For such entities, sharing threat intelligence can be instrumental for monitoring changes in the threat landscape and predicting major cyber threats that might have a disruptive effect on society. With cyber threats and incidents with potential disruptive effect on society we among others mean threats and incidents a) that affect many organisations with (potentially) very serious consequences for these organisations, and/or b) that have a cascading effect resulting in disruption of one or more critical infrastructures. For example, large scale malware infections, affecting many different organisations, or incidents with cascading effects, such as a disruption at an electricity supplier, that causes problems for a telecom service provider that on turn causes problems for a financial service. For establishing situational awareness on cyber threat and incidents with large-scale societal disruptive effect specific data needs to be shared not typically needed for increasing the resilience of individual organisations.

In this paper we investigate how we can leverage from cyber security information sharing infrastructures to gain early insight into the potential effects of cyber threats and the effects of cyber incidents on a national scale. In particularly, cyber threats and incidents that might have a disruptive effect on society. Furthermore, in this paper we will discuss what information needs to be shared and how this can be done using the dominant threat intelligence sharing standards. How to actually establish the desired insight out of the collected information is not addressed in this paper.

2. Approach

2.1 Sharing infrastructure

In our model for sharing threat intelligence we distinguish two types of parties:

1. Computer Security Incident Response Teams (CSIRT) at public and private organisations, and
2. Security Intelligence and Coordination Centre (SICC), such as the NCSC.

The CSIRTs will generally be the consumers of threat intelligence, but can also be producers of threat intelligence from their internal sources. The CSIRTs may share this information with the other parties in the community using the threat intelligence sharing infrastructure. The SICC proactively produces, collects and shares cyber threat intelligence for the community and provides the infrastructure for sharing the threat intelligence. In addition, the SICC has the responsibility to create situational awareness of the threat landscape for the community and to early detect threats and incidents affecting several parties in the community. In case of a national SICC, such as the NCSC, the detection will be focused on gaining early insight into cyber threats and incidents with nation-wide disruptive effects and potential to have a disruptive effect on society.

For the purpose of creation of situational awareness and early detection we assume a so called Hub and Spoke sharing model. This is a model where one organisation, functions as the central clearinghouse for information, referred to as the hub. The hub coordinates the information exchange between partner organisations, which are referred to as spokes. Spokes can produce and/or consume information from the hub. Other sharing models may also be used, but for practical reasons Hub and Spoke is more suited for our objective, since within the Hub and Spoke model the SICC will act as the HUB and have a central role in the exchange of information. See for more information on Hub and Spoke and other sharing models the website of TAXII [1]. In our model the SICC facilitates the hub and also acts a as spoke for production and consuming threat intelligence.

2.2 Sharing information for increasing situational awareness

In our model we assume that organisations receiving threat intelligence are sharing relevant information on that threat intelligence in relation to their organisation with the SICC. For the remainder of this paper we will assume that the SICC is the producer of the threat intelligence and that the CSIRTs will report back to the SICC on that threat intelligence. Furthermore, we assume that the threat intelligence contains Indicator of Compromise (IOC) (e.g., IP addresses of and file hashes of malware), information on the attack methods (i.e. details of observed attacker Tactics, Techniques and Procedures (TTP)) or on the attacker campaign. We distinguish the following information that a CSIRT may report back:

- *Number of hits on an IOC*—this will increase the situational awareness of the SICC on the active usage of the attack method.
- *Potential impact of the threat for the organisation*—this will increase the situational awareness with respect to the severity of the threat for the organisations. The SICC can use this information to assess the potential level of damage this threat could cause.
- *Incident*[1] *related to the particular threat and/or IOC*—this will inform the SICC of successful use of the attack method and will thereby increase the situational awareness of the SICC on the active usage of the attack method.
- *Incident related to the particular threat and/or IOC & the impact to the organisation*—in addition to the previous, this will also inform the SICC of the damage and/or disruptions caused by the incident.

We are aware that reporting incidents and information on the impact of these incidents in particularly is not something that organisation will easily do. Breach notification laws (e.g. those in the Directive on Privacy and Electronic Communications (E-Privacy Directive) from 2009, and in the EU's General Data Protection Regulation [17]) may introduce mandates to report certain types of incidents, but this is not the motivation that we propose for our purpose. We rather hope that the information collected by the SICC will create a new situational awareness that has added value for the whole community. However, the benefit analysis for sharing information is not the focus of our research presented in this paper.

Current initiatives such as the NDN are needed to realise the first steps in information exchange. Current focus is on exchanging indicators of compromise and "count" of the number of sightings. This is a very good first indicator that something is happening but what the effect is on services rendered by individual organisations is not immediately clear. With the ability to share the effects (or impact) is needed to get an insight to determine if and what the (potential) impact is on other (societal) processes.

To illustrate the differences we take the analogy of weather radar. In this analogy an indicators of compromise is the type of downpour (e.g. rain). The sighting is the actual downpour (e.g. amount of rain) and the impact is the related damage at a certain location (e.g. damage to a server due to leakage). The trick with cybersecurity

[1] In this context an incident is a single or a series of unwanted or unexpected security events that have a significant probability of compromising business operations. A security event is an identified occurrence of a system, service or network state indicating a possible breach of security policy or failure of controls, or a previously unknown situation that may be security relevant [16].

is that there is an ever increasing types of downpour and not a lot of experience in what the average impacts are when the downpour materialises. So there needs to be a "translation" from sightings to impact information.

3. Methods and discussion

For the realisation of a threat intelligence sharing infrastructure that supports the automated exchange of information, we have looked at multiple tools (e.g. MISP, Soltra Edge), standards and formats (e.g. IODEF, OpenIOC, STIX). The most promising standards for a threat intelligence sharing infrastructure are CybOX [2], STIX [3] and TAXII [1]. They have been developed under coordination of The MITRE Corporation and have very strong momentum in adoption by industry leaders and threat intelligence communities, such as the FS-ISAC. In the following section we will give a brief introduce in STIX and in particularly introduce some of the structures we intend to use. Next we will assess how the information for increasing situational awareness can be expressed using STIX, and what information needs to be added.

3.1 Brief overview of STIX

The most promising standards for threat intelligence sharing infrastructure are CybOX, STIX and TAXII. Structured Threat Information eXpression (STIX) provides a language to represent cyber threat information in a structured manner. For our purpose STIX is very interesting since it not only provides for a structure approach to format indicators of compromise (i.e. Indicators), but also for a wide set of additional contextual information regarding threats (e.g., adversary Tactics, Techniques and Procedures; Exploit Targets; Threat Actors; Campaigns; and Courses of Action), and for incidents. STIX uses Cyber Observable eXpression (CybOX) for the specification of events or stateful properties in an Indicator that can be observed in a system or on the network. Trusted Automated eXchange of Indicator Information (TAXII) is a set of services and message exchanges that enables sharing of cyber threat information across organisation and between products/services. TAXII is the preferred method of exchanging information represented using STIX.

Our main considerations to use STIX as a basis for further elaboration are, that it is becoming a de facto standard for automated cyber threat information exchange and that it can be used to convey a wide range of threat information. We focus on the STIX packages Indicator and Incident. An Indicator describes a set of observable characteristics or events on a system or network that indicates to adversary activity. The Indicator may also contain contextual information regarding its interpretation, handling, test mechanisms for detection, likely impact, sightings, etcetera. The STIX package Incident is used to convey information of a distinct instance of an adversary activity and/or attack affecting an organisation. It may include structured information on the Incident such as reporter, responder, victim, affected assets, status, attributed threat actors, intended effect and an impact assessment.

3.2 Using STIX for increasing situational awareness

The interaction described above between the SICC and the CSIRTs can be easily mapped to STIX formatted documents. When the CSIRT receives a STIX Indicator containing a new threat, the CSIRT can assess the information and determine the potential impact of this threat to the organisation. The CSIRT may report some of the information from this assessment to the SICC by producing a STIX Indicator with *Likely_Impact*. The STIX indicator document could either be a copy of the received STIX Indicator amended with the *Likely_Impact* information, or a new STIX Indicator with

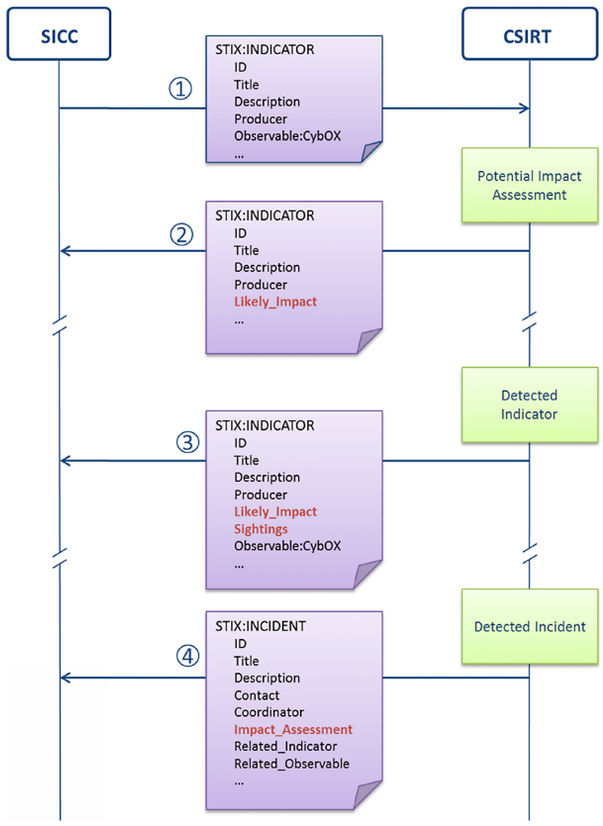

Fig. 1. Interaction between SICC and CSIRT for increased situational awareness

the *Likely_Impact* a reference to the initial Indicator using *Related_Indicators*. This STIX Indicator is only sent to the SICC.

When the organisation has used the observables from the initial STIX Indicator to detect the described adversary activity, the CSIRT may report to the SICC the detection of the observables to detect the described adversary activity. The CSIRT can produce a STIX Indicator with information on the *Sighting* including the *Related_Observables*. Again the STIX indicator document could either be a copy of the received STIX Indicator amended with the *Sighting* information, or a new STIX Indicator with a reference to the initial STIX Indicator using *Related_Indicators*. The CSIRT can report each sighting individually, or report all sighting over a particular period. Note that reporting sightings may cause a large amount of reports to be sent to the SICC. Therefore we suggest that the CSIRT will only report sighting when the SICC has asked to report sightings for that particular STIX Indicator.

If the detection leads to a security incident affecting the organisation, the CSIRT can report this to the SICC using a STIX Incident. To reference to the initially received STIX Indicator, this STIX Incident may contain *Related_Indicators* and/or *Related_Observables*. In addition, the STIX Incident may even contain information on the impact the security incident has *Impact_Assessment*. In Fig. 1 the above described STIX based interaction between SICC and CSIRT to increase situational awareness is depicted.

Although it is possible to map our communication needs to STIX, it is necessary to note that STIX has not been developed with this kind of reporting use case. This manifests itself in the different options how to report on a receive STIX Indicator to the SICC. Above already two options for reporting the sighting using STIX Indicator were described. In addition, it is also possible to report the sighting

Table 1. Impact type and stixVocabs

Impact type	Example	stixVocabs	Enumeration example
Impact on assets	Consequence for asset	ImpactRatingEnum	None—There was no impact. Minor—There was a minor impact. Moderate—There was a moderate impact. Major—There was a major impact. Unknown—The impact is not known.
	Timewindow in which an asset is affected	LossDurationEnum	Permanent—The loss is permanent. Weeks—The loss lasted for weeks. Days—The loss lasted for days. Hours—The loss lasted for hours. Minutes—The loss lasted for minutes. Seconds—The loss lasted for seconds. Unknown—The loss duration is not known
	Effect on security functions of an asset	LossPropertyEnum	–Confidentiality –Integrity –Availability –Accountability –Non-Repudiation
Impact on services	Time window in which services are affected	LossDurationEnum	See above for assets
Impact on business operations Loss (direct and/or indirect monetary) From ISO: impacts on the organisation's business operations. Please note, this is different than impact on services.	Monetary, what are the costs for a department or organisation as a whole Image (how badly is the organisation affected in the media) Example: ISO/IEC 27035: Impact on business operations: cost of recovering business to normal operation and other negative effects of the information security incidents, including loss of profit and/or opportunity.	ImpactQualificationEnum	Insignificant—The impact is absorbed by normal activities. Distracting—There are limited "hard costs", but the impact is felt through having to deal with the incident rather than conducting normal duties. Painful—Real, somewhat serious effect on the "bottom line". Damaging—Real and serious effect on the "bottom line" and/or long-term ability to generate revenue. Catastrophic—A business-ending event. Unknown—The impact qualification is unknown.

in a STIX Incident. Moreover, MITRE has provided guidance on the difference between STIX Indicator and STIX Incident [4]:

- use an Incident if you're describing something that was observed at a point in time for use in analysis or to track history over time;
- use an Indicator if you're conveying detection guidance (things to look for and potentially alert on).

Based on this it is more logical to report the sighting in a STIX Incident. We are not in favour of this approach since many organisations distinguish between security events and security incidents, and the STIX Incident is intended for reporting a single incident and thus limits the possibility to report sightings in an aggregated manner.

Another shortcoming in STIX for the communication needs is the ability to convey (potential) impact information that is necessary for increasing situational awareness. The *Likely_Impact* in the STIX Indicator and *Impact_Assessment* in the STIX Incident are typically intended for local use and typically not to be shared with other parties. In particularly, *Impact_Assessment* has fields intended for conveying impact information to be shared internal, such as *Direct_Impact_Summary* (to characterise asset losses, business mission disruption, and response and recovery related costs), *Indirect_Impact_Summary* (to characterise losses such as loss of competitive advantage, level of impact based on brand or market damage, increased operating costs, legal and regulatory costs), *Total_Loss_Estimation* (to specify total estimated financial loss for the Incident), *Impact_Qualification* (to specify subjective level of impact).

3.3 Required impact information

In our research we looked for usable impact information based on the objective to extend threat intelligence data models with specific information to increase situational awareness and predicting cyber threats that might have a disruptive effect on society. Our approach is to use impact information as a means to report the effects of an incident on the organisation.

Based on recent incidents we can assess what type of impact information is most usable for gaining insight in the societal impact of security incidents. In for example the Dorifel case [5]—ransomware that hit thousands of computer systems on networks in particularly

Table 2. Possible extensions to stixVocabs

Impact type	Example	Possible extension to stixVocabs	Reference/example
Impact on services	Which sector is impacted	SectorEnum	See NACE, or OASIS CIQidentity
	Impact on service	OutageEnum Or DisruptionEnum	Complete (no network) partial (50 % of the voice connections are disrupted. Or 50 % of total bandwith is available).
	Critical services affected	ServiceEnum linked to sector(s)	See North American Product Classification System (NAPCS). Sector specific enumeration of services. Voorbeeld uit ENISA document:112 Emergency service
	How is the service affected	Enumeration for impact on sector specific service	Service specific extension of ImpactRatingEnum
Impact on users	Number/percentage of affected users	"user percentage" or "user minutes"	50 % of service users cannot make calls. 80 % of normally consumed call minutes cannot be delivered in a specific time interval.

of municipalities in the Netherlands in 2012—the impact was reported in various ways. One was the potential impact on information (related to the possible leakage of personal data). A second type was the impact on the amount of effort needed to remediate the infection and its consequences on the computer systems. A third type was the impact on the primary processes of in specific cases the municipalities. Some municipalities had to close some or most of their offices, impacting the services to the general public due to the infection. The later type of impact information was most useful for gaining insight in the societal impact of the security incident.

As the previous example shows the types of impact that could be reported can vary tremendously. Also, these types of information were not reported to the NCSC in a structured manner, but came from amongst others news reports. In order to identify how impact can be reported in a more structured way we did an assessment of available data types that are described in incident management standards and other documents. The following documents were taken into account:

- NIST speciation's [6] and [7]
- The Open Group document [8]
- Multinational Alliance for Collaborative Cyber Situational Awareness document [9]
- ENISA document [10]
- Vocabulary for Event Recording and Incident Sharing document [11, 12]
- ISO/IEC 27035 document [13]

When looking at the (potential) impact information that is given in these documents we found that the use of impact information in traditional security management implementations is to describe the impact for the organisation itself. This means that impact is often described in terms of impact on loss of revenue, extra manpower needed, extra investments in technology etcetera to solve the issue.

In some cases, the impact information is described in terms of impact on (information) systems itself. The best examples for this can be found in the ENISA document which for instance gives impact on telecommunication services. ENISA makes the distinction in impact on the continuity of supply of services and impact on the security of users and interconnected networks. In more detail impact is described in terms of "outage" or "disruption" and depending on what is affected can be reported in terms of complete (e.g. no network) or partial (e.g. a percentage of phone calls dropped in a certain time frame). Other examples include the reporting on the impact on percentage of affected users or user minutes.

Although in the ENISA documents we find some examples, we also see that essential information is lacking in order to be able to determine social impact. For instance, whether the impact on the service is limited to a specific region.

3.4 Challenge/obstacles in organisations

The way impact information is described and used within an organisation's risk management system, may be a potential barrier for sharing impact information. Impact information that is established for internal use to determine the impact on the financial continuity of a business is commercially sensitive. Therefor we see a need for a common understanding of impact information that is both useful for the SICC to increase situational awareness and acceptable for organisation to be shared.

Another barrier for automated information exchange is that there is no clear enumeration of services and their related impact types. Although some enumeration for sectors is already incorporated in STIX [14] via the OASIS CIQidentity [15]. Per sector the typical services, such as described in the ENISA document are still lacking. Which means that it might be possible to determine in which sector an impact has materialised, but it is not possible to determine what services are impacted and in what way.

3.5 Ideas on extending STIX

Not all barriers discussed above can be solved by extending STIX. With the focus on the ability to automate the sharing of cyber-

security incident impact information, some extensions to STIX are envisioned. One is to extend the enumeration of sectors with enumeration of services per sector. The following step is to extend on the specific impact per service. Looking at the example given by the ENISA document this could be by adding:

- Impact based on affected users
- Impact based on percentage of the service affected

This could be extended with information of the affected geographic region that is affected.

Within STIX this data could be implemented by using Likely_Impact which relates to the potential impact given that an event or threat might occur. The actual impact might be reported using Impact_Assessment.

Table 1 shows some examples in which the stixVocabs can be used to enumerate impact related information. It should be noted that in the table assets and services are distinguished. Assets are used by an organisation to deliver its services. Within STIX™ the difference between assets and services is not explicitly made, and both are given in AssetTypeEnum. In AssetTypeEnum the VERIS framework is used. Examples of AssetTypes within STIX™ are: Media, ATM, broadband, DHCP, Gas terminal, Laptop, Media, Mobile phone, Peripheral, POS terminal, Kiosk.

In Table 2 some examples for extension of StixVocabs are given based on the analyses described above.

4. Conclusions

In this paper we showed that it is possible to leverage from threat intelligence sharing infrastructures to gain early insight into the large scale effects of cyber threats and incidents. We showed what type of information can be reported to a so called Security Intelligence and Coordination Centre (SICC) to increase situational awareness. In particularly, the number of sightings of a previously shared indicator of compromise, potential impact on the organisation of a previously shared threat, and incident with impact on the organisation and reference to shared threat intelligence.

It is possible to map this type of communication to STIX. However, the data fields available in STIX to report (potential) impact information are mainly focused on reporting the impact information internally in the organisation. In order to share the desired impact information we need to extend STIX.

Currently there is no clear enumeration of services and their related impact types for automated information exchange. This is type of information is necessary to be able to assess and detect societal disruptions due to cyber security incidents in an early stage. As shown in the examples it should be possible to extend the stixVocabs with additional enumerations that supports this type of information sharing. The next step is to extend the required enumerations and make them specific for sector related services.

References

1. MITRE (2014): Trusted automated eXchange of indicator information. [ONLINE] Available at http://taxii.mitre.org/.
2. MITRE (2014): Cyber observable eXpression. [ONLINE] Available at http://cybox.mitre.org/.
3. MITRE (2014): Structured threat information eXpression. [ONLINE] Available at http://stix.mitre.org/.
4. MITRE (2014): Incident vs. indicator. [ONLINE] Available at http://stixproject.github.io/documentation/idioms/incident-vs-indicator/index.html.
5. National Cyber Security Centrum (2013): Cybersecuritybeeld Nederland, CSBN-3. Den Haag: NCSC, Ministerie van Veiligheid en Justitie.
6. National Institute of Standards and Technology (2012): Computer security incident handling guide NCSC. NIST: Ministerie van Veiligheid en Justitie.
7. National Institute of Standards and Technology (2011): Information security continuous monitoring (ISCM) for federal information systems and organizations.
8. The Open Group (2009): Risk taxonomy. Berkshire: The Open Group.
9. Multinational Alliance for Collaborative Cyber Situational Awareness (2013): Information sharing framework v2.4. Multinational Alliance for Collaborative Cyber Situational Awareness.
10. European Network and Information Security Agency (2013): Technical guidance on the incident reporting in Article 13a. ENISA.
11. VERIS Community: Impact [VERIS Community]. 24 12 2012. [Online]. Available: http://www.veriscommunity.net/doku.php?id=impact [Accessed 17 March 2014].
12. VERIS Community: Overview [VERIS Community], VERIS, 2012. [Online]. Available: http://www.veriscommunity.net/doku.php?id=overview. [Accessed 29 04 2014].
13. ISO/IEC 27035-2: Information technology—security techniques—information security incident management—Part 2: Guidelines to plan and prepare for incident response, ISO 2014.
14. MITRE (2014): Victim targeting by sector. [ONLINE] Available at http://stixproject.github.io/documentation/idioms/industry-sector/.
15. OASIS (2014): OASIS customer information quality (CIQ) TC. [ONLINE] Available at https://www.oasis-open.org/committees/ciq/.
16. ISO (2014): ISO/IEC 27000:2014 Information technology—-security techniques—information security management systems—overview and vocabulary.
17. http://en.wikipedia.org/wiki/Security_breach_notification_laws.

Authors

Frank Fransen
received his M.Sc. degree from Eindhoven University of Technology, The Netherlands, in 1995. He then joined KPN Research as a researcher in the area of ICT security and smart card systems. Currently, he is employed as a senior scientist in the information security group of TNO, The Netherlands. His current interests include security of mobile communication systems, threat intelligence management and cyber security of smart energy grids. Frank has produced several publications and is the (co-)inventor of about 10 patents. Frank has participated in many standardisation fora, among others 3GPP SA3 on mobile network security and the Dutch counterpart of ISO JTC1 SC27 on IT security techniques.

Andre Smulders
M.Sc., CISSP is an expert in the field of information security with more than 14 years of experience. Since 2005 he has been working at TNO as senior business consultant security for a variety of contractors in both public and private sectors. In his role as expert in the area of ICT security and security governance, he is co-author of the book "Foundations of Information Security—based on the ISO27001 and 27002", various articles and most recently the TNO publication "Networked Risk Management". He has been chair for different expert groups and speaker on national and international symposia.

Richard Kerkdijk
M.Sc., has been active in the field of information security since 1997. His present position is that of senior security consultant at TNO, an independent R&D and consulting organisation in The Netherlands. Richard fulfils a strategic advisory role towards various companies and government bodies, with emphasis on clients in the telecoms and finance industry. Throughout the years, Richard has been involved in a wide variety of security and fraud related projects, both as specialist and project leader. Current topics of interest include security monitoring and incident response, threat intelligence sharing and utilisation and cyber security in the broader sense. Mr. Kerkdijk holds the position of vice-chair in the ETIS Information Security WG, a forum for collaboration and information exchange among the Chief (Information) Security Officers of European telecoms providers.