Transport Canada Transports Canada

MARINE SECURITY OPERATIONS BULLETIN

No: 2021 - 001

REPORTING REQUIREMENTS CONCERNING CYBER SECURITY THREATS, BREACHES, INCIDENTS AND VOLUNTARY REPORTING OF CYBER- RELATED SUSPICIOUS ACTIVITY

PURPOSE:

The purpose of this bulletin is to provide guidance on the methods by which reporting requirements related to cyber security threats, breaches and incidents and the voluntary reporting of cyber-related suspicious activity can be fulfilled.

This bulletin supports and should be read in conjunction with MSOB 2014-001 *Clarification of Transport Canada (TC) marine security mandatory threat, breach and incident reporting requirements* and MSOB 2016-002 *Suspicious Activity Reporting*. This bulletin applies to stakeholders subject to the *Marine Transportation Security Regulations* (MTSR), the *Domestic Ferries Security Regulations* (DFSR), the *Cruise Ship and Cruise Ship Terminal Security Measures*, the *Security Measures respecting Designated Tall Ship Events* and the *Security Measures Respecting Tall Ships and Marine Facilities that Interface with Tall* Ships – hereafter referred to as "regulated stakeholders".

Additionally, this bulletin provides information and awareness on other resources that regulated stakeholders can use in the event of a cyber-security event, such as the Canadian Centre for Cyber Security (Cyber Centre); and, information on other federal reporting requirements for industry stakeholders particularly concerning cyber security breaches that involve privacy, as set out by the Office of the Privacy Commissioner of Canada (OPC).

BACKGROUND:

The marine industry has become increasingly dependent on cyber technology for nearly every aspect of marine transportation. The proliferation of cyber systems across the marine transportation system continues to transform the risk landscape, with cyber-related risks representing a growing portion of all security risks faced by maritime stakeholders. As a result, the timely and consistent reporting of cyber-related threats, breaches and incidents and cyber-related suspicious activity is vital to understanding, improving and maintaining the security of Canada's marine transportation system.

The ambiguous nature and number of cyber security threats, breaches and incidents makes it difficult for stakeholders to determine what to report. For example, due to the interconnectedness of cyber systems, assessing the impact/seriousness of any threat, breach or incident is not always obvious. Furthermore, determining what to report can be further exacerbated by a cyber security attack's ability to hide its true intent and the sheer volume of potential and realized events. Transport Canada recognizes these reporting challenges and expects that regulated stakeholders

to use their best judgment, experience and the guidance materials provided in this bulletin when reporting events.

Transport Canada treats all reports of security threats, breaches and incidents, as well as suspicious activities, as sensitive security information - whether physical or cyber. Once reported, Transport Canada shares the information as required, with the appropriate law enforcement agencies and public safety partners based on any identified risks to Canada. Information from reports of security threats, breaches, incidents as well as suspicious activities are also analyzed by Transport Canada to identify trends and patterns; to make decisions when addressing potential threats that may be identified; and, to assist those responsible for the development of regulated stakeholders' security assessments.

DEFINITIONS

MSOB 2014-001 *Clarification of Transport Canada (TC) marine security mandatory threat, breach and incident reporting requirements* provides interpretational guidance for the definitions of a ***security threat***, ***security breach***, and ***security incident*** as articulated in Sections 1(1) of the MTSR and DFSR. MSOB 2016-002 *Suspicious Activity Reporting* provides a definition of the term ***suspicious activity.***

***Cyber security threat*:** A type of *security threat* (see MTSR Section 1(1), DFSR Section 2(1), and MSOB 2014-001) – any suspicious act or circumstance, respecting the collection, disruption, denial, degradation, or destruction of an information system resource or the information itself, that could compromise the security of a vessel, marine facility, port, domestic ferry, domestic ferry facility, or interface's network and the information the network carries.

Cyber security breach: A type of *security breach* (see MTSR Section 1(1), DFSR Section 2(1), and MSOB 2014-001) – a violation of a security measure, rule or procedure that results in unauthorized access to data, applications, services, networks and/or devices but that does not result in a security incident.

***Cyber security incident*:** A type of *security incident* (see MTSR Section 1(1), DFSR Section 2(1) and MSOB 2014-001) – an event during which the security of a vessel, marine facility, port, domestic ferry, domestic ferry facility, or interface is compromised as a result of an attack which modifies, destroys, deletes or renders unavailable any computer network or system resource.

Cyber-related suspicious activity: A type of *suspicious activity* (see MSOB 2016-002) – an activity involving a vessel, marine facility, port, domestic ferry, domestic ferry facility, or interface's cyber systems that falls outside of a normal pattern of behavior (i.e., if the precision, volume, persistence or sophistication of the activity/attack is out of the ordinary). For instance, while malicious cyber activities such as phishing attacks and network scanning are often part of the normal information technology landscape, more targeted (e.g. targeted phishing "Spear phishing" campaigns) or intense attacks (e.g. a marked increase in network scans) are more rightly classified as suspicious activities. Determining cyber-related suspicious activities will always be context dependent.

Cyber security event – A cyber security change that may have an impact on vessel, marine facility, port, domestic ferry, domestic ferry facility or interface's operations including mission, capabilities, or reputation. Cyber security events are inclusive of cyber security threats, breaches and incidents, as well as cyber-related suspicious activities.

DIRECTIVE:

Regulated stakeholders should use this bulletin when evaluating and reporting cyber security threats, breaches and incidents. Regulated stakeholders may also use this bulletin when evaluating and reporting cyber-related suspicious activity.

1. For port administrations, marine facilities, occasional-use marine facilities, and domestic ferry facilities

Regulated stakeholders shall report all cyber security threats, breaches and incidents occurring at a marine facility, a ferry facility, a port, or an interface between a vessel or a tall ship and a marine or ferry facility or another vessel to appropriate law enforcement agencies, Transport Canada and, if applicable, the port administration, as soon as possible after they occur so that an investigation can be conducted. Regulated stakeholders shall also review and verify that all security plans, procedures, and technical safeguards are up to date and not connected to the cause of the cyber event.

Regulated stakeholders are encouraged to report cyber-related suspicious activity to Transport Canada as soon as feasibly possible.

2. For Canadian flagged vessels, domestic ferries and tall ships

Cyber security threats and cyber security incidents shall be reported to the master, the company security officer, the appropriate law enforcement agencies, Transport Canada and, if applicable, the port administration, as soon as possible. For Canadian flagged vessels subject to the MTSR's that are operating in foreign waters, these reporting requirements shall be met regardless of the location of the vessel. Cyber security breaches shall also be reported to Transport Canada as soon as possible after they occur, regardless of the location of the vessel, ferry or tall ship. Regulated stakeholders shall also review and verify that all security plans, procedures, and technical safeguards are up to date and not connected to the cause of the cyber event.

Regulated stakeholders are encouraged to report cyber-related suspicious activity to Transport Canada as soon as feasibly possible. In the case of vessels following the International Maritime Organization (IMO) *Guidelines on Maritime Cyber Risk Management* (MSC-FAL.1/Circ.3), the requirements set out in the MTSR (i.e., Sections 212, 218 and 229(k)), supersede those guidelines. This approach is consistent with the IMO's Maritime Safety Committee's recommendation that the International Ship and Port Facility Security Code should not require a vessel to establish a separate cyber security management system that operates in parallel with a vessel Safety Management System (MSC 101/WP.1/Add.1); and, reaffirms Resolution

MSC.428(98) and the organizational requirements for administrations to ensure that cyber risks are appropriately addressed.

REPORTING GUIDANCE

1) Administer internal impact assessment of the cyber security event.

While it could be difficult to determine the scope and impact of a cyber security event (and if it meets the definition or threshold to be considered a threat, incident or breach), we encourage regulated stakeholders to consider cyber systems that perform a critical function or are related to security safeguards, processes or procedures outlined in the facility or vessel security plan.

In determining whether the cyber security event should be reported, the regulated stakeholder should consider whether the event:

- Circumvented any established security policy, safeguard, measure or procedure, regardless of the nature of the event (intentional or accidental) and regardless if the security of a vessel, facility, port or installation was affected;
- Had the potential to threaten or affect the integrity of the security posture of the regulated facility or vessel or the integrity of assets and infrastructure;
- Could impact vessels, facilities or ports or their operations;
- Could impact national security or the general security and ongoing functioning of the marine transportation system and its infrastructure;
- Requires a liaison and coordination with the regulatory, security or intelligence community;
- Necessitates a discussion with or the attendance of a TC Marine Security Inspector (to provide regulatory guidance);
- Triggered a need to implement alternate security arrangements; or
- Impacted the ability of a regulated stakeholder to fully implement its marine security plan.

Transport Canada recognizes that no description could cover all possible events and therefore expects that regulated stakeholders will use their best judgment, experience and guidance materials provided in determining when to report events. When uncertain whether a cyber security event should be reported, regulated stakeholders are encouraged to err on the side of caution and report the event.

ANNEX A provides a non-exhaustive inventory of cyber security events – cyber security threats, security breaches and cyber-related security incidents – including reporting guidance for each event.

2) **Report all cyber security threats, breaches, and incidents to appropriate law enforcement organization; and, Port administration or Company Security Officer (as applicable) in accordance with regulatory requirements (MTSR, DFSR).**

ANNEX A provides a non-exhaustive inventory of cyber security events – cyber-related security threats, security breaches and security incidents – which should be reported (and to whom).

3) **Report cyber security threat, breach, incident or cyber-related suspicious activity to Transport Canada in accordance with regulatory requirements (MTSR, DFSR).**

It is advised that cyber security threats, breaches, incidents and cyber-related suspicious activities be reported to the Transport Canada National Situation Centre (TCSC) at the contact information below:

Transport Canada National Situation Centre

1-888-857-4003 (toll free within Canada/U.S.) or 1-613-995-9737 (all other areas).

The TCSC operates 24 hours a day, 7 days a week.

Follow up reports or documentation may be emailed to Sitcen@tc.gc.ca with a carbon copy to your TC regional marine security office.

Stakeholders should provide the following information when making a report:

- Name of organization/source information (name, telephone number, e-mail address);
- Date and time of incident;
- Date and time of reporting (if applicable, when information is received from a secondary source);
- Location of incident (province, city, marine facility name, location on the facility or vessel where the incident occurred, Port Authority name, if applicable;
- Description of activity (describe cyber event, networks affected, impact on security, etc.);
- Actions taken by the reporting stakeholder;
- Who else was informed; and
- Other relevant information.

The details of any security vulnerabilities revealed by the event need not be discussed during an initial report. Transport Canada will work with the reporting source, and with other appropriate authorities, to investigate and respond to the report.

4) Consider reporting cyber security events to local law enforcement agencies, as well as the Canadian Centre for Cyber Security.

Regulated stakeholders and others are encouraged to report cyber security events to both local law enforcement agencies and to the Cyber Centre. Transport Canada recommends stakeholders consider reporting cyber security events to law enforcement agencies within jurisdiction, as they have an interest in hearing from those directly impacted by cyber security events. This is so an investigation can be opened, which can only be initiated by the affected parties. Additionally, opening an investigation related to the cyber security event is an important and critical step in possibly determining the source and cause of the attack, and may assist in preventing future ones of a similar nature.

As part of Communications Security Establishment, the Canadian Centre for Cyber Security (Cyber Centre) is Canada's authority on cyber security. The Cyber Centre is the single unified source of expert advice, guidance, services and support on cyber security. The Cyber Centre operates 24/7, with staff onsite 15/7, and serves critical infrastructure organizations in Canada.

The Cyber Centre's role is to assist critical infrastructure organizations in Canada to protect their cyber systems from compromise. They offer assistance in preventing, mitigating, and detecting malicious cyber activity to stakeholders free of charge.

Port security officers, marine facility security officers, vessel and tall ship security officers, operators of vessels, facilities, ports and industry personnel who notice unusual activity on their systems, discover a malware infection or are the targets of other kinds of cyber events are encouraged to report these activities to the Cyber Centre. Information shared with the Cyber Centre is anonymized before it is shared with other partners and is only shared with the permission of the affected organization(s). The Cyber Centre also encourages reporting any event where the sharing of information within the broader cyber community would be of value to mitigate cyber risks to Canada and to Canadians.

Canadian Centre for Cyber Security (Cyber Centre)

Toll Free: 1-833-292-3788

contact@cyber.gc.ca

5) Report to the Office of the Privacy Commissioner of Canada as required.

Regulated stakeholders should familiarize themselves with the new reporting requirements set by the Office of the Privacy Commissioner of Canada (OPC). As of November 1, 2018, businesses (both large and small) subject to the Personal Information Protection and Electronic Documents Act (PIPEDA) are required to:

- Report to the Privacy Commissioner of Canada any breaches of security safeguards that involves personal information which may pose a harm to the affected individuals,
- Notify affected individuals about those breaches, and
- Keep records of all breaches.

A breach of security safeguards is defined in PIPEDA as the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 of PIPEDA, or from a failure to establish those safeguards.

There is a PIPEDA breach form accessible through the Office of the Privacy Commissioner of Canada (OPC) website. There is also specific guidance and other training material on the website, including tips for containing and reducing the risks of a privacy breach and securing personal information.

ADDITIONAL INFORMATION:

The Cyber Centre can assist Canadian critical infrastructure organizations in the marine transportation sector to protect their cyber systems from compromise.

Partnering with the Cyber Centre will provide industry stakeholders access to:

- Experts in cyber security, for mitigation advice and support;
- The Cyber Centre's malware detection and analysis capability;
- A cross-sector, pan-Canadian, and global perspective on various types of malicious activity;
- Awareness products on trending cyber security issues;
- The Cyber Centre's unique understanding of the cyber landscape in Canada; and
- Assistance in the prevention of cyber events by allowing anonymized information to be shared with other partners.

To become a partner and subscribe to the distribution list, please contact: contact@cyber.gc.ca

Some Cyber Centre products are available through the Cyber Centre's public website. Additionally, the Cyber Centre has a secure Community Portal for its partners in both public and private sectors. You can also find additional information and guidance as well as alerts and advisories issued by the Cyber Centre on potential, imminent or actual cyber threats, vulnerabilities or incidents affecting Canada's critical infrastructure.

The Community Portal contains all of the Cyber Centre's various products, including those not posted to the public website, as well as other tools designed to enhance incident mitigation for partners. The Portal also offers a series of separate sites (also known as sub sites) organized by sector or community of interest.

QUESTIONS:

Any questions, concerns or comments about this MSOB can be addressed to the Director, Marine Security Operations by e-mail at dirops.marsec-sumar@tc.gc.ca.

_____

Malick Sidibé
Director, Marine Security Operations
4 March 2021

ANNEX A – CYBER SECURITY EVENTS

When assessing whether a cyber event should be reported or not, it is important to consider its impact, both real and potential, to critical cyber systems. Below is a list of possible scenarios.

Examples of a cyber event with a large impact could include:

- A large, sustained distributed denial of service (DDoS) attack against a critical cyber system, causing it to become unavailable to operators, resulting in loss of a critical function.
- A sophisticated, targeted attack using a spear-phishing email or watering hole website to infect users resulting in malware being installed on the computer. From here, the malicious actors would then pivot from this computer to traverse the network for further compromise and potentially to exfiltrate data.
- A user clicking on a link or attachment in an email, causing a ransomware attack that encrypts critical files and systems on the network, resulting in loss of a critical function.
- A critical system running a vulnerable version of software that has been recently announced to have an untended security vulnerability that has not been resolved (also known as zero day vulnerability) and is being actively exploited by malicious actors.

Examples of a cyber event with minimal impact could include:

- A sophisticated, targeted attack using a spear-phishing email or watering hole website to infect users resulting in a malware infection. Despite the system having been compromised, if no further exploitation occurred, then the potential impact of the attack is considered to be low.
- Phishing emails with the intent on installing banking credential malware.

Below is a list of reportable cyber scenarios, along with possible methods by which a computer spreads a virus (also known as infection vector). Please note that this list is non-exhaustive and should be used a reference point only.

Reportable Cyber Scenarios		
Vectors	**Examples**	**Definitions**
External/Removable Media	Malicious software spread using infected removable media (e.g. flash drive, CD, or removable hard drives, etc.	
Attrition	Denial of service	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or unwillingly participating in the DoS.

	Ransomware	A computer system or device is infected by malware that restricts access to it and demands that the user pay a ransom to remove the restriction.
	Brute force	Attacker attempts to gain unauthorized access via systematically checking all possible keys or passwords until the correct one is found.
Web	Watering Hole attacks	Malware is found residing on a websites which a group or employee often uses.
	Web application attacks / injection attacks (Code injection: SQL, XSS)	Custom web applications embedded within social media sites are utilized to install malicious code onto computers to be used to gain unauthorized access
	Drive-by download	A drive-by download refers to the unintentional download of a virus or malicious software (malware) onto your computer or mobile device.
Email	Spear phishing attacks	Employees receive a targeted e-mail message that has been crafted to create fake trust and thus lure the victim to unveil some business or personal secrets that can be abused by the adversary.
	Phishing attacks	Employees receive fraudulent emails, where the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy websites.
	SPAM or Unsolicited infected e-mails	Receiving unsolicited, undesired, or illegal email messages that may have an infected attachment or link.
Improper Use	Any incident resulting from a violation of an acceptable use policy.	For example, downloading pirated software onto corporate network, installation of file sharing software, etc.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization	For example, the loss or theft of an employee's laptop, smart phone, or authentication token.
Other	Rootkits	Stealthy types of malware software (e.g. software designed

		to hide the fact that an operating system has been compromised, sometimes by replacing vital executable files) are activated or installed.
	Remote Access Tool (RAT)	Software with remote administration capabilities is infected, allowing an attacker to control the victim's computer.
	Exploit Kits	Software kit designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it, and discovering and exploiting vulnerabilities to upload and execute malicious code on the client machines.
	Viruses/Trojan	A program designed to breach the security of a computer system while ostensibly performing some innocuous function.
	Elevation of privileges	Bugs, design flaws or configuration oversights in an operating system or software application are exploited to gain elevated access to resources.
	Mobile Malware	Malicious software that targets mobile phones or wireless/cellular-enabled tablets and mobile computers, by causing the collapse of the system and/or loss or leakage of information.
	Spyware or deceptive adware	Software that aims to gather information about a person or organization without their knowledge.
	Reconnaissance & Probing	This incident category includes any activity that seeks to access or identify a computer, open ports, protocols, service, or any combination for later exploit. This activity may not necessarily result in a compromise or denial of service.

Term	Definition
Advanced persistent threat (APT)	An adversary that possesses sophisticated levels of expertise and significant resources which pursues its objectives over an extended period of time, adapts to defenders' efforts to resist it, and is determined to maintain a presence on the targeted network.
Botnet	A botnet is a collection of compromised computers ("robots" or "bots") under the control of a malicious actor.
Zero Day Vulnerability	A zero-day (also known as zero-hour or 0-day) vulnerability is an undisclosed computer-software vulnerability that malicious actors could exploit to adversely affect computer programs, data, additional computers or a network.
Crimeware	Malicious software that is covertly installed on computers and has the ability to 'steal' confidential information and send it back to cyber criminals.
Cyber attack	The unintentional or unauthorized access to, use, manipulation, interruption or destruction, via electronic means, of electronic information or the electronic devices or computer systems and networks used to process, transmit or store information.
Cyber security	The body of technologies, processes, practices, and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability.
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the target of, or unwillingly participating in, a DoS attack.
Event	An observable change to the normal behavior of a computer, IT system, environment, process, or workflow that may impact or may pose a threat to the system or data integrity, or safety and security. An event can be upgraded to an incident if it becomes apparent that the change observed has a probable negative impact.
Hacktivism	A combination of hacking activity and activism.
Improper usage	Any activity that violates acceptable computing use policies.
Incident	A single or a series of unwanted or unexpected information security events which have a significant probability of compromising business operations, national security, or public safety.
Malicious code	*Successful* installation of malicious software (e.g. virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
Phishing / targeted emails	A digital form of social engineering that uses authentic-looking, but malicious, emails to request information from users or direct them to a fake website that requests information.
Research (incident type)	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.
Scans/ probes/ attempted access	This includes any activity that seeks to access or identify a computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
Spear phishing	A category of phishing that consists of targeting specific individuals.
Unauthorized access	Any activity whereby an individual gains logical or physical access without permission to a network, system, application, data, or other resource.