RESULTADO DEL WORKSHOP DE IALA: CIBERSEGURIDAD

Ciberseguridad en organizaciones hermanas a IALA

BIMCO

- Reciente publicación de las guías de ciberseguridad a bordo de buques
- De acuerdo con la Res. **IMO MSC.428(98)** Gestión del ciber-riesgo en sistemas de gestión de la seguridad (safety), las compañías marítimas deben incluir la **gestión del ciber-riesgo en el Sistema de gestión de la seguridad (safety)** y no en el plan de protección (security) del buque.
- La gestión del ciber-riesgo debe concordar con los objetivos y requisitos de del **código ISM 1.2.2**.
- Las administraciones deben asegurarse que los ciber-riesgos se atienden convenientemente en los sistemas de gestión de la seguridad (safety) **no mas tarde que la primera verificación anual del documento de cumplimiento de la compañía (Document of Compliance) después del 1 de Enero de 2021**

BIMCO

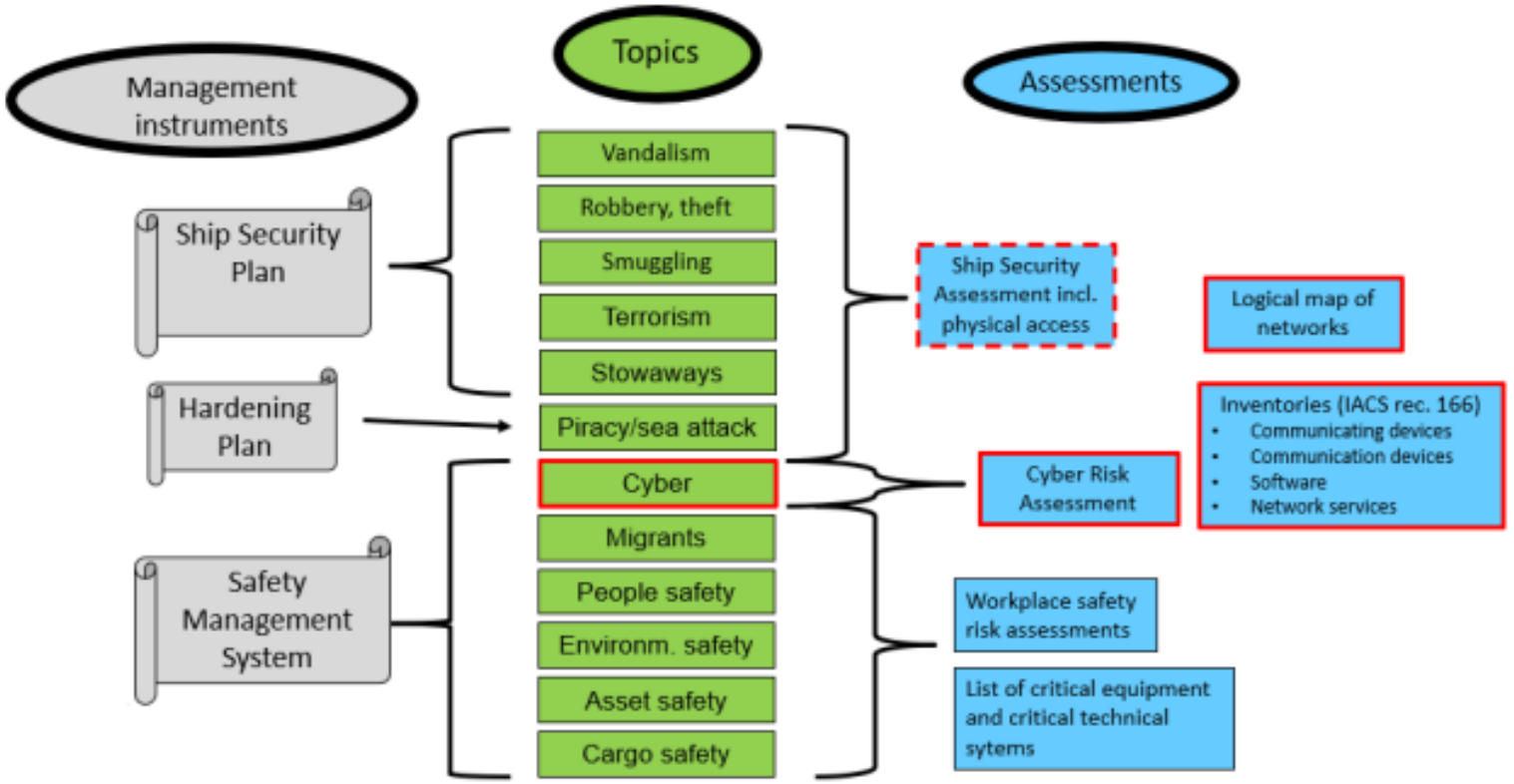


Figure 1 - Structure of the approach from a shipping company on cyber risk managing

BIMCO

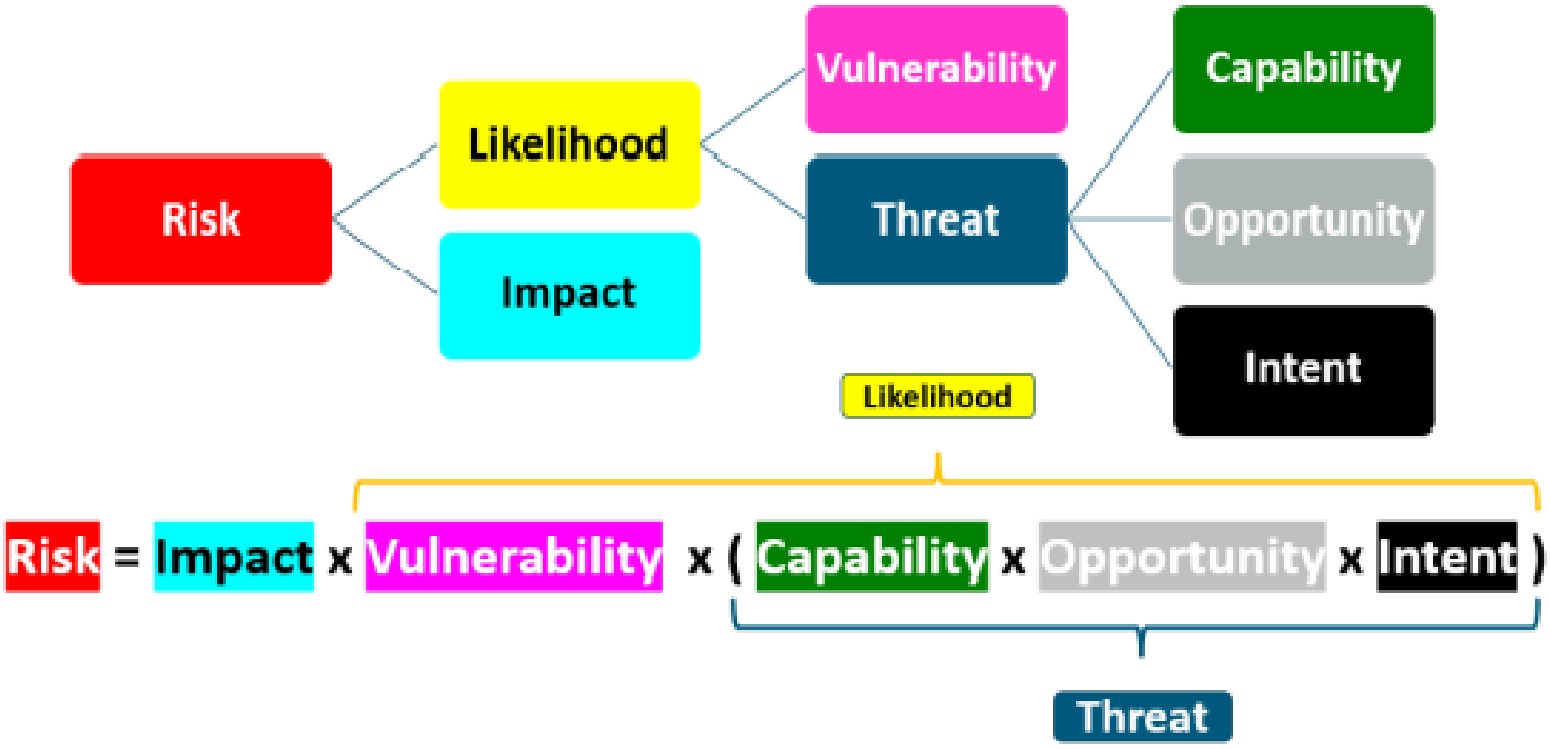
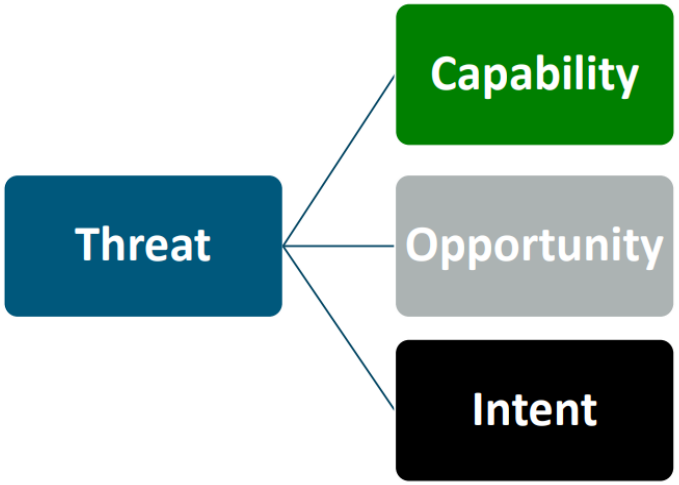


Figure 2 - Risk calculation and breakdown of elements of risks (BIMCO)

BIMCO



- Phishing
- Malware
- Hacking
- Social engineering
- Denial of service

- Internet
- Wifi
- Removable devices
- Physical access

- Financial gain
- Vandalism
- Personal motives
- Political motives

Applicable to
- OT systems
- IT systems

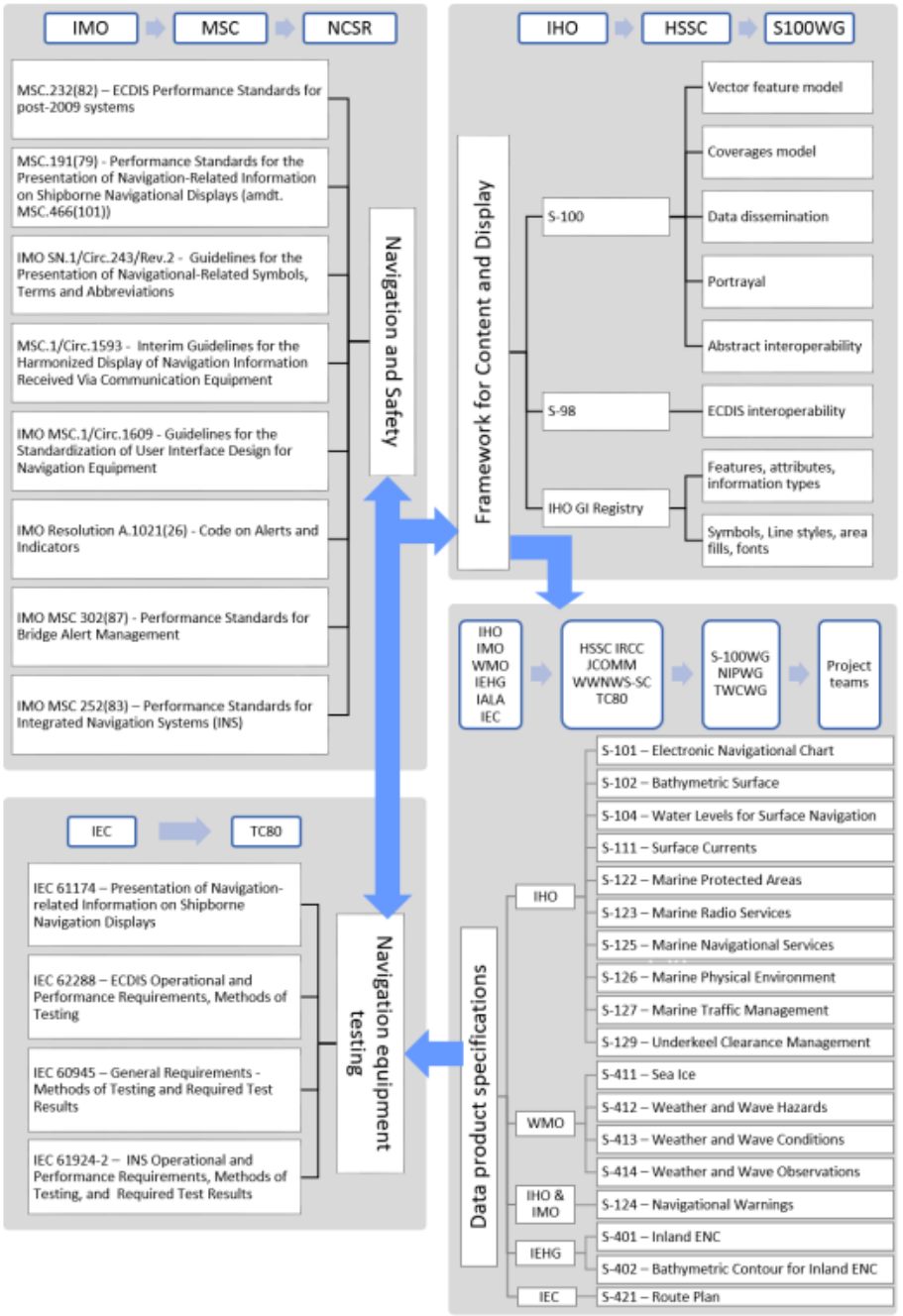
BIMCO establece las siguientes recomendaciones inmediatas:

- Mapear accesos remotos y flujos de datos
- Segregar redes: sistemas críticos, administrador, tripulación, pasajeros
- Proteger el acceso a ordenadores y sistemas a bordo (firewall, administración de contraseñas, puertos de medios extraíbles, control de acceso físico)
- Proteger el correo electrónico y otros sistemas y software de acceso a Internet (antivirus).
- Iniciar la capacitación y concienciación de todo el personal.

IHO

- Información sobre la evolución del estándar para la protección de datos: Integridad de los datos y cómo se implementan en el marco de la S-100 de la OHI, así como también cómo se aplica la ciberseguridad impactando en esa implementación.
- Últimas actualizaciones del Modelo de Datos Hidrográficos Universal de la OHI de la S-100, que es implementado como parte de la nueva generación de cartas electrónicas (más productos, mejorados de la interoperabilidad ...) **S-100 Part 15 se incluye específicamente para la protección de datos de S-100** (cifrado de datos y firmas digitales para autenticación)
- S-100 también será interoperable con varios estándares técnicos para la seguridad / integridad de los datos utilizados en las principales tecnologías de Internet (X509). Para tal fin, se dispondrá de un ECDIS S-100 revisado y homologado.

IHO and AtoN



- Estándares generados en IMO e IEC son inputs para S-100 con el objetivo de que todos los datos importados al ECDIS sean:

→ **digitalmente firmados (autenticación: el origen se puede verificar en el ECDIS) y,**

→ **opcionalmente, algunos de ellos podrían encriptarse para protección de la copia.**

- Por ejemplo, en relación con los datos provenientes de la red AtoN, el proveedor de servicios AtoN sería autenticado por IALA, quien está autenticado internamente por la OHI. Por lo tanto, el esquema de protección de datos de la OHI proporcionará la certificación de identidad de los datos disponibles en el puente.

IHO

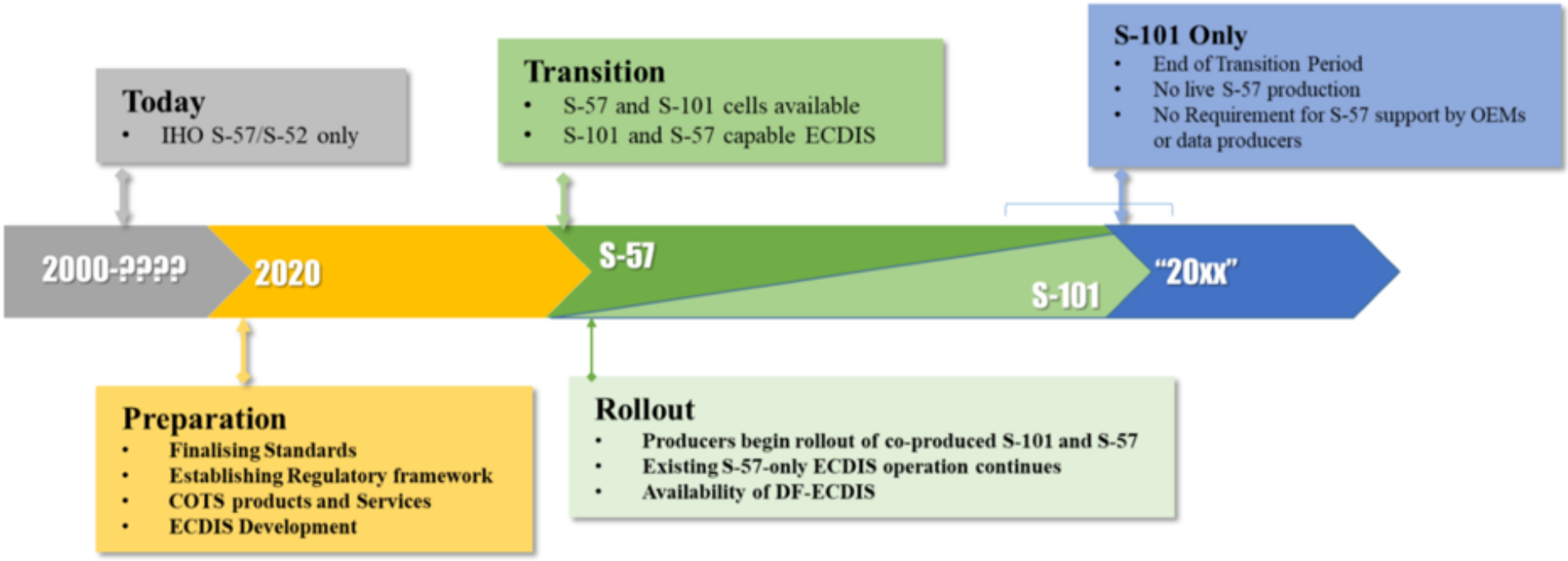
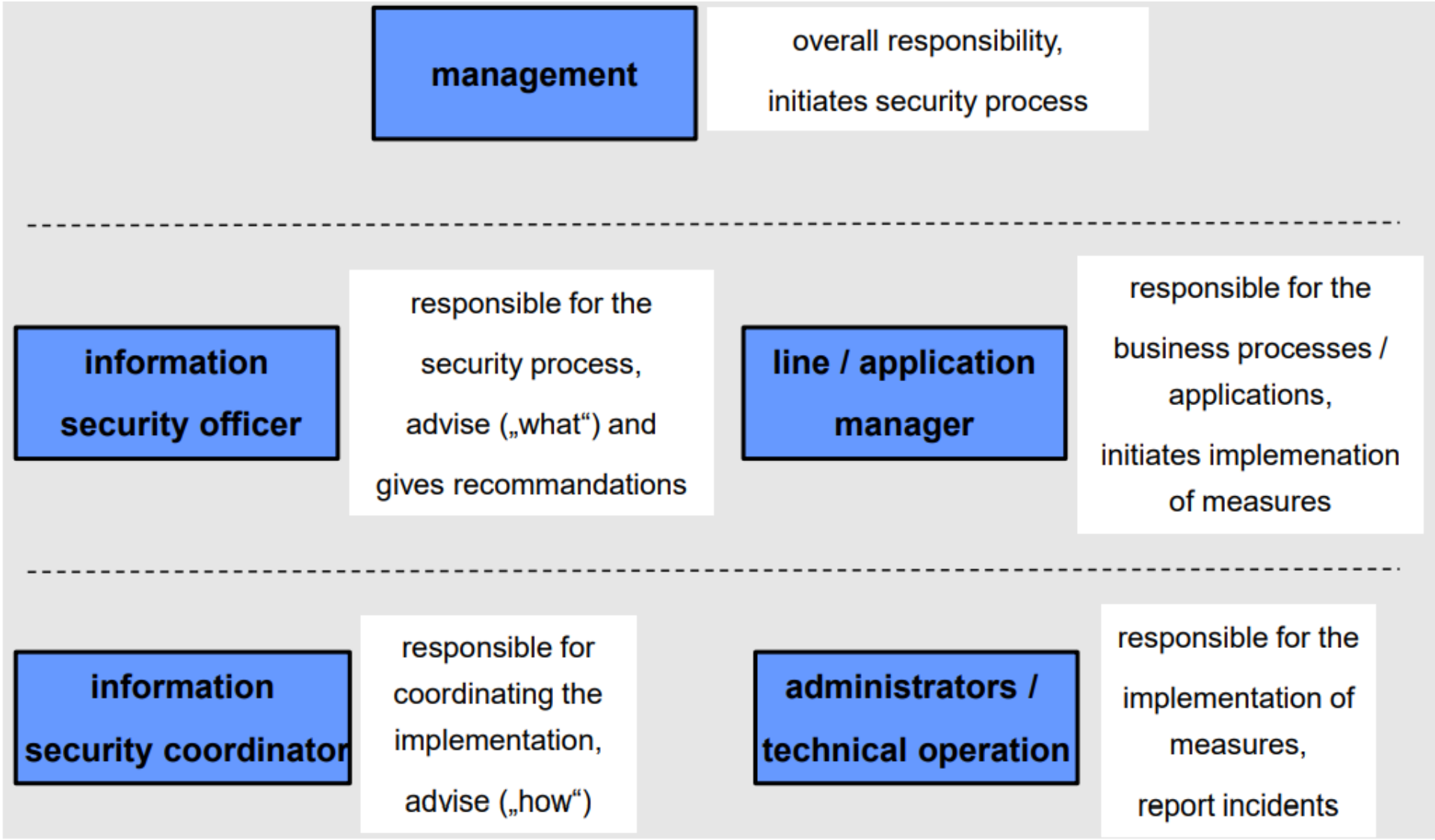


Figure 3 - Roadmap of IHO standards and its implementation on the ECDIS

La última revisión de la S-100 Ed.5 saldrá en 2022 y será la base para la revisión de los estándares de prestaciones de IMO para que ECDIS incluya la S-100.

Medidas preventivas para asegurar la ciber-resiliencia: ejemplo de la Autoridad de vías navegables y transporte marítimo de Alemania



Medidas preventivas para asegurar la ciber-resiliencia: ejemplo de la Autoridad de vías navegables y transporte marítimo de Alemania

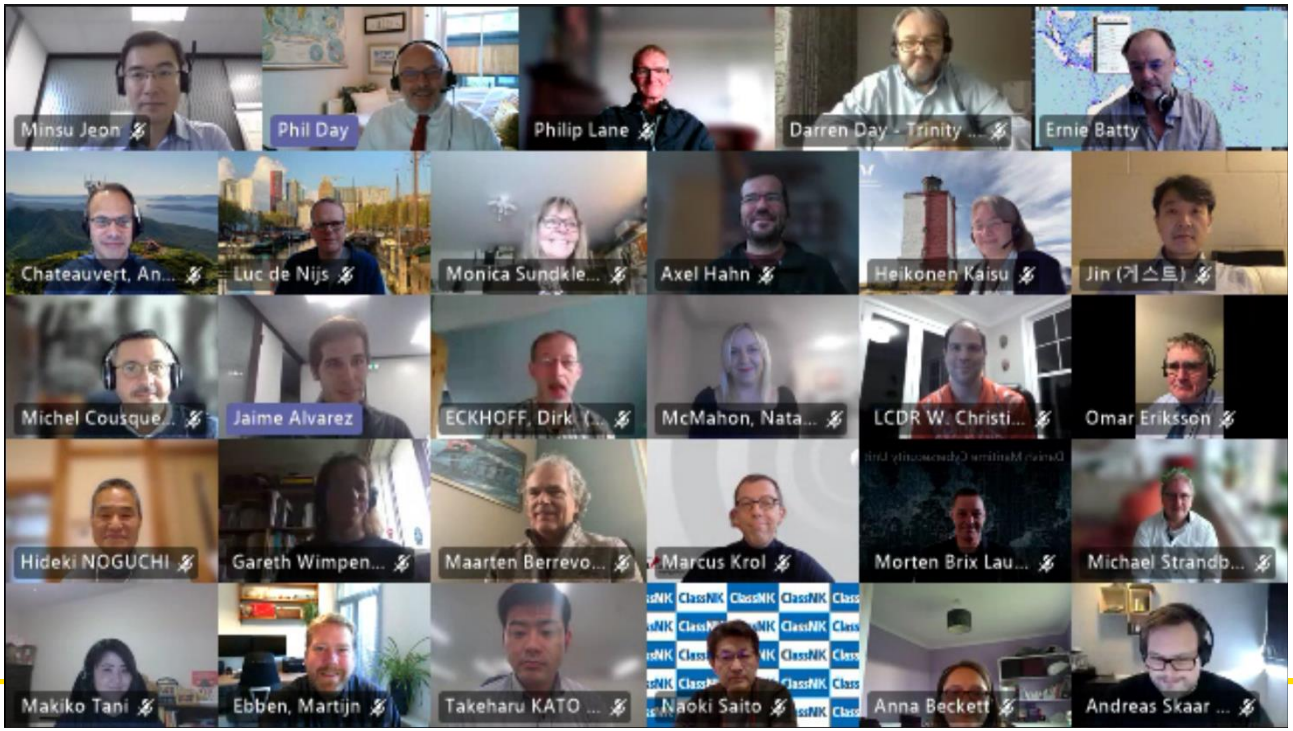
- **Enfoque por procesos**: no solo en la seguridad de IT, desde los procesos comerciales e incluyendo IT, activos, organización y personal). Es necesario definir la criticalidad (a través de niveles de protección de las aplicaciones) y su implicación en los procesos comerciales.
- La implicación de la Gestión de Seguridad de la Información (ISM) también es necesaria y aborda nuevamente algunas funciones y responsabilidades de la organización del personal cuando se trata de una nueva aplicación y/o aplicaciones y sistemas que ya están en uso. **En ambos casos (aplicación / sistema nuevo y en uso), se debe producir y mantener un catálogo de requisitos de seguridad para edificios, servidores, clientes y gestión de cambios.**
- Se establecen dos tipos de requisitos: **requisitos principales** (obligatorios de implementar) y otros requisitos (el riesgo es aceptable, no obligatorio de implementar).
- En cuanto al elemento humano, se sugirieron algunos puntos para concienciar a los empleados sobre el tema de la ciberseguridad (reuniones, información, instrucciones, demostraciones con el fin de incrementar aceptación y comprensión.
- Finalmente, se enfatizó sobre la pregunta sobre el manejo de incidentes de seguridad considerando los procedimientos, la disponibilidad del personal de seguridad, los canales de reporte, el tiempo de acción y las responsabilidades finales y la toma de decisiones dentro de una organización. **La primera respuesta a un incidente debe dar paso a: gestión de crisis / continuidad del negocio / recuperación.**

Sesiones de trabajo

Grupo de trabajo 1 - Medidas y comportamientos procedimentales preventivos

Grupo de trabajo 2 - Medidas técnicas preventivas

Grupo de trabajo 3 - Respuesta a incidentes y recuperación (post-operativo)



Grupo de trabajo 1 - Medidas y comportamientos procedimentales preventivos

- Se consideraron los factores humanos en la ciberseguridad para AtoN y VTS.
- Se identificaron brechas en los procedimientos y la capacitación actuales
- Se propusieron mitigaciones para esas brechas, identificó amenazas y medidas para prevenir interrupciones operativas.
- Se consideró cómo crear y fomentar una cultura de ciberseguridad, donde la ciberseguridad sea reconocida e integrada en el día a día del negocio.

- RECOMENDACIONES:

1. Es fundamental crear conciencia, implementar procedimientos relacionados con la seguridad cibernética, fomentar un buen comportamiento de seguridad cibernética y proporcionar formación periódica;
2. Los roles / perfiles de ciberseguridad y las responsabilidades asociadas deben asignarse en toda la organización;
3. La ciberseguridad debe ser parte de la cultura de gestión en toda la organización y convertirse en un tema permanente de la agenda como un elemento para mantener un ambiente de trabajo seguro y saludable;
4. La seguridad cibernética debe integrarse en la gestión del ciclo de vida de los sistemas.

Grupo de trabajo 2 - Medidas técnicas preventivas

- Se identificaron sistemas vulnerables, propuso mitigaciones y medidas de protección, y propuso trabajo a desarrollar en el alcance de IALA

- Si bien las plataformas y equipos dentro del alcance de IALA están sujetos a las mismas amenazas y vulnerabilidades que los sistemas en el resto del mundo, el WG2 identificó los sistemas de **posicionamiento, navegación y cronometraje (PNT) y el sistema de identificación automática (AIS)** como sistemas particulares donde IALA podría implementar medidas de protección y mitigación.

- **Vulnerabilidad importante: falta de autenticación, autorización y cifrado en muchos de los sistemas dentro del alcance de IALA**. El Grupo consideró que existe una necesidad imperiosa de garantizar que la autenticación esté integrada en los nuevos sistemas y productos.

Grupo de trabajo 2 - Medidas técnicas preventivas

- RECOMENDACIONES:

1. Integridad de GNSS: continuar apoyando el trabajo de ENG WG3 y ENAV WG2
2. Profundizar (a través de la guía de pautas de seguridad cibernética) la importancia de proteger la IT contra las amenazas tradicionales como un objetivo prioritario (objetivo organizacional), antes de encontrar e implementar soluciones para la seguridad AIS (que requiere un esfuerzo de toda la industria).
3. Los miembros reconozcan las capacidades de mitigación y detección de interferencias y suplantación de AIS y GNSS existentes en los componente comerciales, las empleen de la manera más eficaz en sus operaciones y proporcionen una guía sobre cómo protegerse contra otras amenazas similares
4. La necesidad de un esfuerzo de toda la industria, posiblemente iniciado por IALA, sea discutido al más alto nivel de decisión de la organización IALA.
5. Establecimiento de un grupo de trabajo para definir un camino hacia la búsqueda, adopción e implementación de una solución sólida a largo plazo para la autenticación de mensajes AIS.
6. Informar y ajustar los objetivos de ENAV WG 1 (Sistemas de información digital) para incluir la exploración de soluciones criptográficas que apoyarían el uso de PKI en aplicaciones de bajo ancho de banda.
7. Sugerir a ENAV WG1 que debería considerar el documento IEC 63173-2 SECOM (S-100) (dando soporte a la comunicación basada en IP) para admitir otra tecnología de intercambio de datos que no sea IP, p. AIS, VDES, etc., en contacto con el Grupo de trabajo de IEC que trabaja en esto (IEC TC80 WG17).

Grupo de trabajo 3 - Respuesta a incidentes y recuperación (post-operativo)

1. Enfoque y escenarios de continuidad del negocio

• Riesgos asociados a ciberseguridad deben incorporarse en los planes de continuidad del negocio existentes.
• Desarrollo de escenarios para ciber incidentes, en particular para los sistemas AtoN y OT
• Los **sistemas heredados**, especialmente en las operaciones AtoN, deben considerarse, tanto como un riesgo como como alternativa para los sistemas automatizados (informáticos).

2. Mejores prácticas en materia de continuidad empresarial

• La continuidad del negocio debe organizarse en toda la organización.
• Es importante tener **copias de seguridad**, que también pueden ser medios de instalación y / o copias de seguridad de la configuración.

3. Mejores prácticas de respuesta a incidentes

• Se debe establecer una **política clara y un plan de respuesta a incidentes**.
• Deben crearse y cumplirse los documentos de estrategias de escenarios
• Necesidad de análisis y asistencia en la recuperación**, se recomienda un tercero especializado**. Es posible que se necesite cooperación ya que es posible que un tercero no tenga un conocimiento profundo de los sistemas AtoN.
• acciones para realizar la respuesta a incidentes pueden afectar la operación AtoN y desencadenar acciones de continuidad del negocio, anticipar resultados
• Un incidente cibernético debe evaluarse mediante un **ejercicio de lecciones aprendidas**, para mejorar los planes y estrategias.

Grupo de trabajo 3 - Respuesta a incidentes y recuperación (post-operativo)

4. Las acciones priorizadas dentro del plan de continuidad y para la respuesta a incidentes cibernéticos

- Análisis de riesgo e impacto
- Planificación y preparación
- Decidir contratar un MSP (Proveedor de servicios gestionados) / CERT (Equipo de respuesta ante emergencias informáticas

5. Medios para informar y compartir información sobre incidentes cibernéticos

- IALA podría considerarse un recurso de **ISAC (Centro de análisis e intercambio de información)**
- Modificar la recomendación R1009 de la IALA existente sobre recuperación ante desastres para incluir aspectos de seguridad cibernética
- Modificar la directriz G1120 de la IALA existente sobre recuperación ante desastres para incluir aspectos de seguridad cibernética
- Desarrollar una nueva guía o recomendación para aspectos específicos en la respuesta y recuperación de incidentes cibernéticos, posiblemente incluida la gestión de crisis y la gestión de la continuidad del negocio, para los operadores AtoN y las autoridades de VTS, a medida que las operaciones se desvíen de las mejores prácticas genéricas de la industria.

Además de estos temas, el grupo desarrolló un documento informativo “Inventario de mejores prácticas en respuesta a incidentes y recuperación y continuidad del negocio” (ANEXO E) para todos los Comités de IALA como referencia útil para el trabajo futuro de los Comités e invitó al taller a aprobar el trabajo para presentarlo con el informe del taller.

El informe del workshop de ciberseguridad será un input para los siguientes Comités y a disposición de todos los miembros de IALA

Los nuevos flujos de trabajo sobre ciberseguridad en operaciones AtoN (incluido VTS) empezaran a tomar forma en la siguiente temporada de comités (Marzo Abril 2022)

Es importante que los países de habla hispana integren dichos grupos de trabajo para no solo recopilar las recomendaciones y guías pero también participar en la definición de los procedimientos, avances y tecnologías en el alcance de la ciberseguridad

Esperamos veros a partir de Marzo 2022

ENG15	07 March 2022 - 11 March 2022	IALA Headquarters	Book now
Preparing for a PAWSA workshop	07 March 2022 - 18 March 2022	Online by distance learning	Book now
ENAV29	14 March 2022 - 18 March 2022	IALA Headquarters	Book now
MCP Identity Management and Security Seminar	19 March 2022	IALA Headquarters	Book now
ARM15	21 March 2022 - 25 March 2022	IALA Headquarters	Book now
LAP23	29 March 2022 - 30 March 2022	IALA Headquarters	Book now
VTS52	04 April 2022 - 08 April 2022	IALA Headquarters	Book now