Risk Management

The following will produce a report that should support the organisation of a Risk Management Plan (RMP) from the perspective of a Cyber Security Manager (CSM).A RMP requires an analysis of CBORD's services in order to extract a substantial level of comprehension of the design of CBORD. This should then enable a CSM to identify and discuss potential vulnerabilities that in turn reveal risks that help determine the severity and context in and around a threat against CBORD[5].

This artifact will be broken up into three sections. The first section will present information in four parts. The first part will introduce standards (and clauses within said standards) alongside methodology's and describe their relevance to CBORD. The second part will include the identification of business assets paired with the risks they're associated with. The knowledge will be collected from parts one two to formulate a RMP that will outline scenarios within the context of CBORDin the third part. The last part will justify the remedy's that are selected to alleviate risks using an argument that is supported by other potential risk treatments that are not included in the RMP. Section A should provide a CSM a general perspective to CBORDdesign in order for them to put in place instructions that anticipate the event of a threat.

Half of Section B will describe systematic activities that can be implemented by the relevant stakeholder(s) under particular circumstances. Put forth in a fashion that justifies the Risk Managements Plan's handling of regulatory/legal issues. The second half of Section B will further discuss the degree the RMP is tailored to CBORD. Section C will echo the structure of Section B with a focus on the technological elements.

Section A

1

The ISO 31000 (2018) is a General Risk Management (GRM) claim that services need an assessment to be performed frequently if it intends to remain updated sufficiently. It has a reputation recognised by security experts that span internationally [3].

Here it will be paired with CBORDwho offer a service that uses NII (non-Intrusive Inspection) technologies to carry out boarder control[1].

Scope

The service of IIS requires niche technology that needs to keep up with the growing volume of trade[2]. Because The ISO 31000 (2018)can provide a framework without having to be innately fixed to any specific field it can grow and adapted in response to CBORD's service demands. The scope can involve processes within a context than can span from non-sector to industry specific if need be. The scope enables the activities that implement a RMP to be carried out at a rate that matches the life cycle of CBORDservices. This will help the Risk Management Planto protect CBORDfrom threats whilst keeping the organisation identity consistent by retaining its values and enhancing the quality of CBORD's performance[4] [1].

Terms and definitions

A CSM will need to predict the occurrence of risks at a level of accuracy in the context of CBORD's objectives. This can be done by adopting a means to measure and categorise risks and the threat they pose. To do this affectively the vocabulary pulls from multiple relevant sections documented in the International Electrotechnical Commission in order to be rich enough for the Risk Management Planto deliver

its information. This will enable a CSM to develop a protocol that is comprehensive enough to counter risk events as well as produce a means to locate the source of a threat to reduce likely-hood of the potential negative impact.

The demands on CBORD's services will require the organisation to evolve. For the terms and definitions to adhere to that evolution, the vocabulary of the Risk Management Planwill likely require continuous revision from the CSM. This will enable them to maintain an idea of how likely an event will take place, at what cost and to who if a vulnerability is actioned[4].

Principles

For the standard of the processes that exist at CBORD's to be optimal. The work of the Risk Management Planneeds to be lead by principles that enable the a CSM to deter threats with positive affect and minimal waste in time, and resources. The results of CBORD's objectives are not guaranteed.

For security violations to be of less concern. The right principles should help prepare CBORDfor a range of a number of threats[4]. This requires the culture at CBORDto nurture knowledge among staff so that risk management activity can be performed alongside the day to day workflow. If that is the case a CSM can recognise when the Risk Management Planis tailored to CBORD.

framework

support vision for company and effective leadership. established with a plan/policy ensure distrubtion of resourcess

ISO 31000 recommends a top down approach (design) from lead by managament to execute organise decision makeing and acivities that implement successfull risk managment. distributing responsibility on all involved. this also includes evaluation in order to report results and lead towards consinuous improvment woven into Org's process tha deliver seriveces.

Process

manifest as dedicated meetings, accesiable comprhesive documentation and drills nurture knowledge over a range of skills sets. systematic actions actions that implement the framework. procedures exercised on the occirance/idetification of a risk analysis judge time and degree of impact.

The preparation for information security risk a security manager may apply a widely known threat modelling methodology called STRIDE[**?**].

STRIDE(computer security threats)

Information risk clauses informed by ISO 27001:2013 along side risk management design

Policy for information security - Clause 5.2

this be the recommended starting point. manefest as a document. tailored to company. requires effective communication throughout organisation and its activities shared vision express the benefit of info security Top down management. and implementation

Context of Org - clause 4

establish "internal/external" environment. boundriesro resources, storage, priveledges accessibility The impact on objectives. established risk management proceseses (systematic protect against misuse of information componants of ISMS will also support this

2

CBords business assets will include the tangile and intangable items to mention This will include vehicles, real estate, digital devices, office items and intellectual property. A security manager may need to have access to a balance sheet that will list and value C-BORDs itemized business assets [**?**].

Threats around country boarders need to be detected: - nuclear chemicals using found using photofission [6]. - relocable/ restricted space [**?**]

Take establishments such as USA - homeland security UK [**?**]

Use cases to describe scenario: Ports using, fixed installments or relocatable operation context [1] Advanced Radiation Management / Next Generation Cargo X-Ray / Evaporation Based Detection / Tagged Neutron Inspection / Photo-fission

And land borders using mobile operation context.

Clause 4.1 Understanding the organization and its context

[**?**]

Clause 4.2 Understanding the needs and expectations of interested parties

[**?**]

Clause 4.3 Determining the scope of the information security management system

[**?**]

Clause 4.4 Information security management system

[**?**]

Clause 5.2 Information Security Policy

[**?**]

Clause 6.2 ISO 27001 Information Security Management Standard

[**?**]

CBORDS explains the possession of their "Toolbox" which consists of the following[5].

Gamma Detection Sub-systems (C-BORD Advanced Detection Systems). This comes in the form of Mobile Detection Systems, Radiation Portal Monitors, Relocatable Portal Monitors.

Sealed items are monitored with a Passive Neutron Tagged Neutron Inspection System[5]. A photofission detection module for the detection of SNM (Special Nuclear Material). Evaporation based detector tools.

Its possible to assume the interlectial property might consist of [**?**]. The data collected during and after C-BORD carries out their inspection processes. For example this might include radiation detection data, X-ray images enhanced user feedback and the presense of illicit items.

In order to describe the associated threats against busniess assets a security manager will likely need to have a record of the value of a given asset. It may be either appropriate or even neccessary to ensure this is tracked against time as the value is due to modify against this attribute [6].

The fright will also come the form of containers and vehcles the likes of trucks, cars, vans and trains. The contents won't belong directly to C-BORD, however a security manager will likely have to specifify what degree C-BOARD will want to be responsible for the fright contents through out its service.

If a threat is acted up this might have implications against CBORDs brand which is perhaps appropriate to consider as the face of the organisation which will want to hold up a good reputation and positive relationship with their customers [24].

Given the business assets mentioned above its possible to put forth some assumptions involving the processes within C-BOARD and any associated risks (vulnerabilities) that might appear against the mentioned assumptions.

That can help see threats [6]

Create controls to manage those threats

Avaliability of a C-BOARD process authrized parties for integirity(assets modified by authorised)

...monitoring fright data. This might happen in real time by an authorized user.

Artifacts scans in the wrong possesion.

3

The following will detail CBORDS risk management processes for a security manager to carry out in order perform a risk assesment that will allow for an analysis of identifable threats and include a considerations to migitate them [10].

"Objectives"[10] The following will consider C-BORD from a high level perspective for an overview of the NII service it provides

"reliable detection of radioactive material, explosives, chemicals, drugs, and tobacco hidden in cargo containers."

"to increase detection of illicit or dangerous material"

"deliver new capabilities against critical operational requirements and constraints"

"Increased throughput of containers per time unit"

"Reduced need for costly, time-consuming and dangerous manual container inspections"

"Lower false negative and false positive alarm ratios"

Risk Identification [10] "A risk, or uncertain event, can be a positive or negative condition that has a financial, operational, or reputational impact."[10] "review digital assets such as systems,

Authentication 2 factor thing passwords unaurthrised access. packet sniffing

networks, VPN - resources to shared files Clouds - store priverladges firewalls pin that changes (grey fob thing)

software, databases, spreedsheets emails

data menfest as the in the software like dbms. Files like spreedsheets,

devices, laptops/desktop computers. Mobile phones - messages. "toolbox" location, the screen facing

Customers? fright content

"Cataloging these assets then allows the team members to identify risks to the assets[10]

Risk Assessment [10]

Risk Analysis [10]

Risk Tolerance [10] And the reasons for the one described above ... possible to design/visualise a model of the business workflow that includes security

Assumme from different perspectives of the architecture.

User perspective

Attacker perspective.

Because the risk assesment and managment plan complys with ...

4

Justification of risk treatments based on appropriate criteria and consideration of alternatives.

User interaces to for authorised CBOARD employes. Assuming this will likely require passwords that could potencially give way to access from an unauthurised user. Using STRIDE we might look out for Spoofing. In which case ...

We could assume the same case could lead to an Elevation of Privilege...and this could mean...

The same vulnerability it might seem natural to beware of the lileyhood of activity including Tampering with data.

ability to identify nuermous suspicious activity.

a varity a potencial threatening acts could plant malware potencially that captures data if assume devices are woking on a network denial of service spying

adminsiterator of users could remove account. remove access the account has to files.

Recovery if an unautheroised user has knowledge of perhaps illicite items or not. inform bodies in assication with items. prosectute crime

limit network endpoints

At this point the standard/methodolgy has been selected for reasons brought forth by the management plan. Establish a criteria that its possible to justify the following risk treatments.. An alternative might be..

to counter/respond to risks/risk senarios, the plan includes ...

it could be possible to use....

Its then possible for security management to distribute responsibility to the necessary roles so a reporting procedure is in place when a threat is acted upon [22].

People involed

characteristics of good tech "core copatencies of organisation

Section B

1

Legal issues related to the security that I feel we effect the service are ...

to ensure a design in place that makes standard set legally to attempt to mitigate risks and respond to security breaches[12]

the needs to consider the variations in laws for data privacy and protection. organised on a national level down to provicial area[19].

EU for example is legally obligated to act according to General Data Protection Regulation GDPR. on securuty breach 72 hrs to information Commissioner Office (ICO)[12]

where Alabama requres up to 10 days [21]. or in the US different states[12].

the state of cycber space evolves services will need to be updated frequently [20].

Affect the service in this way...

Uphold hold governing bodies that specifiy a standard standard[13].

UK currently specified by mcss[14]

specifiies incident response[15]

Recognise where costs in time in money [11]

Copyright to protect artififacts [6]

Patent to protect tangable objects[6] Patent for software

Patent holder to manfest as a body to liability occurs[6]

A trademark trade secret (reverse engineering) - for on novel techniques (algortithms) cbord uses [6] however there are decompilers/disaseemblers- infer code design[6]

need for an effective response [12]
notify legal bodies within a time frame after a breach [12]

2

Apropriateness/feasibility of proposed methods to tackle issues identified. ...a recommendation for how to resolve those issues might include...
training people [18]

Section C

Based on recent/current research, cycber security related techiical areas worth recommending to the company management for consideration for furth work or inclusion in the service are ... ...These areas merit consideration because...

1

2

Bibliography

[1] C-BORD(2022,Feb.25). *P*roject Overview. cbord-h2020.eu/page/project-overview.php. [Accessed: 25 Febuary 2022].

[2] C-BORD(2022,Feb.25). *P*roject Overview. https://tfig.unece.org/contents/NII-technology.htm. [Accessed: 25 Febuary 2022].

[3] Feb.20) ISO(2022. *I*SO Risk Management[online]. pivotpointsecurity.com. https://www.iso-3100-risk-management.html[Accessed:10febuary2022]. [Accessed: 21 Febuary 2022].

[4] ISO(2022.Feb.22). *I*SO Risk Management-Guidelines[online]. pivotpointsecurity.com. www.iso.org/obp/ui/iso:std:iso:31000:ed-2:v1:en[Accessed:22Febuary2022]. [Accessed: 22 Febuary 2022].

[5] R.Barrus(20, Aug,25). *W*hat Is Theat Modeling. pivot point security[online]. https://www.pivotpointsecurity.com/blog/what-is-threat-modeling-and-how-does-it-differ-from-risk-asses [Accessed: 10 febuary 2022].

[6] Pawel Sibczynski, Andrzej Dziedzic, Krystian Grodzicki, Joanna Iwanowska, Tymoteusz Kosiński, Michał Matusiak, Marek Moszynski, Lukasz Swiderski, A. Syntfeld, D. Wolski, Frédérick Carrel, Amelie Grabowski, Matthieu Hamel, Frederic Laine, Adrien Sari, Alessandro Iovene, and Carlo Tintori. Comparison of prompt and delayed photofission neutron detection techniques using different types of radiation detectors. 11 2016.