Managing Cyber Security Risk

A direct link to Digital Risk
and Business Reputation

CAPT. ZARIR IRANI

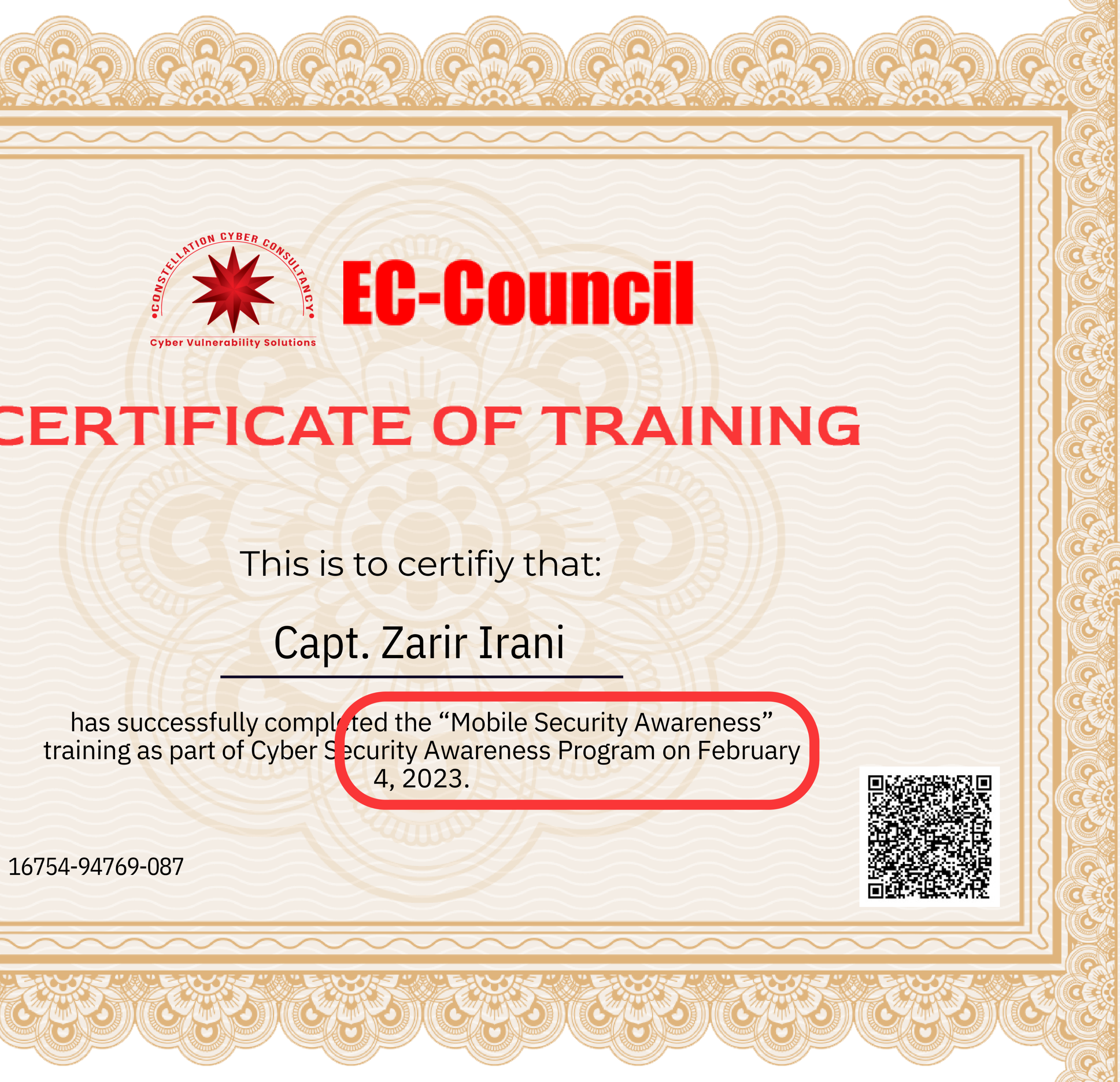
MBA. HON FIIMS, FICS, FNI, HCMM, ASSO. CII, NAMS-CMS

CONSTELLATION MARINE SERVICE

CONSTELLATION CYBER CONSULTANCY
Cyber Vulnerability Solutions

How many have taken part in cybersecurity awareness training in the last month?

Show of Hands✋



CONSTELLATION CYBER CONSULTANCY

Cyber Vulnerability Solutions

EC-Council

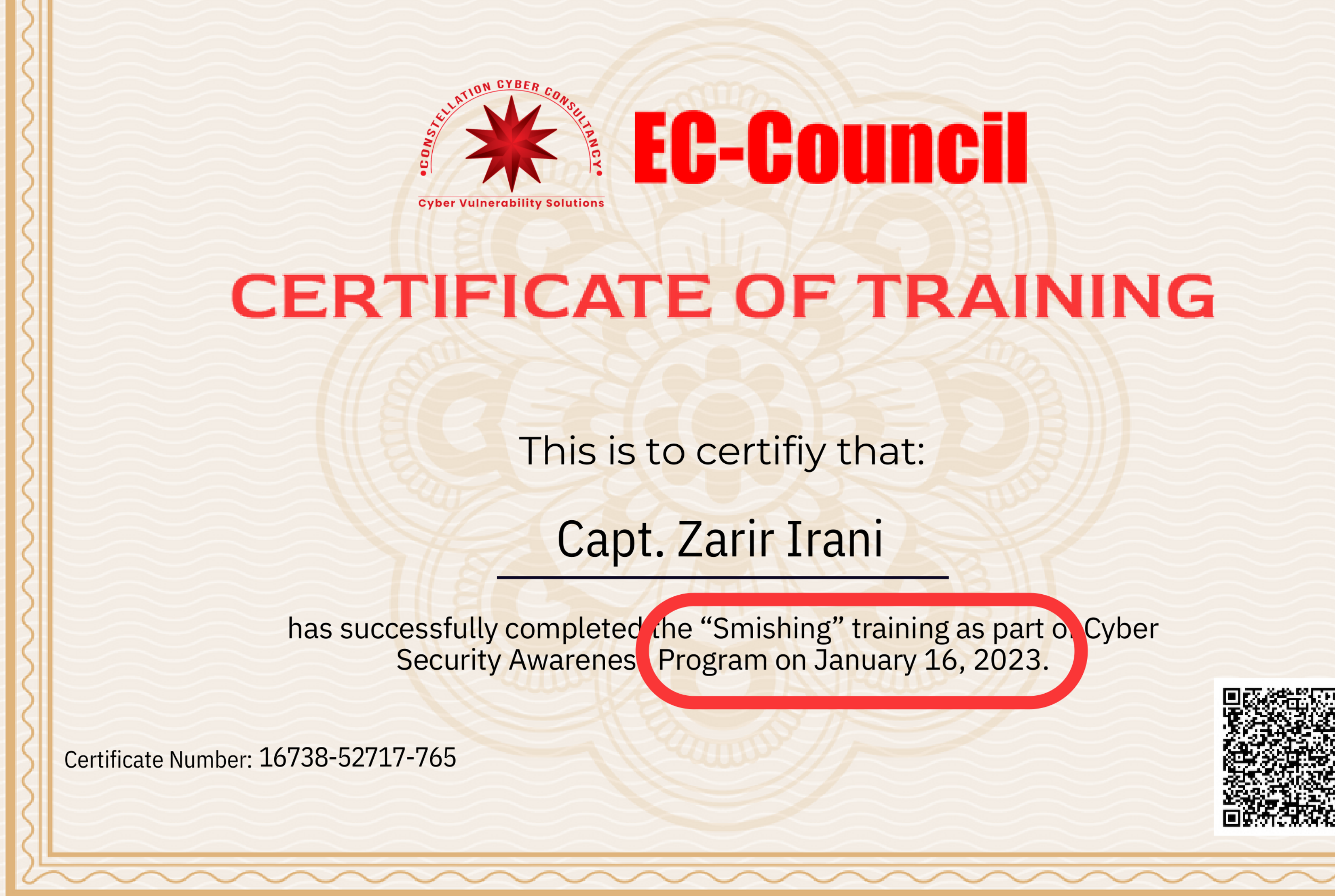
CERTIFICATE OF TRAINING

This is to certifiy that:

Capt. Zarir Irani

has successfully completed the “Mobile Security Awareness” training as part of Cyber Security Awareness Program on February 4, 2023.

16754-94769-087



CONSTELLATION CYBER CONSULTANCY

Cyber Vulnerability Solutions

EC-Council

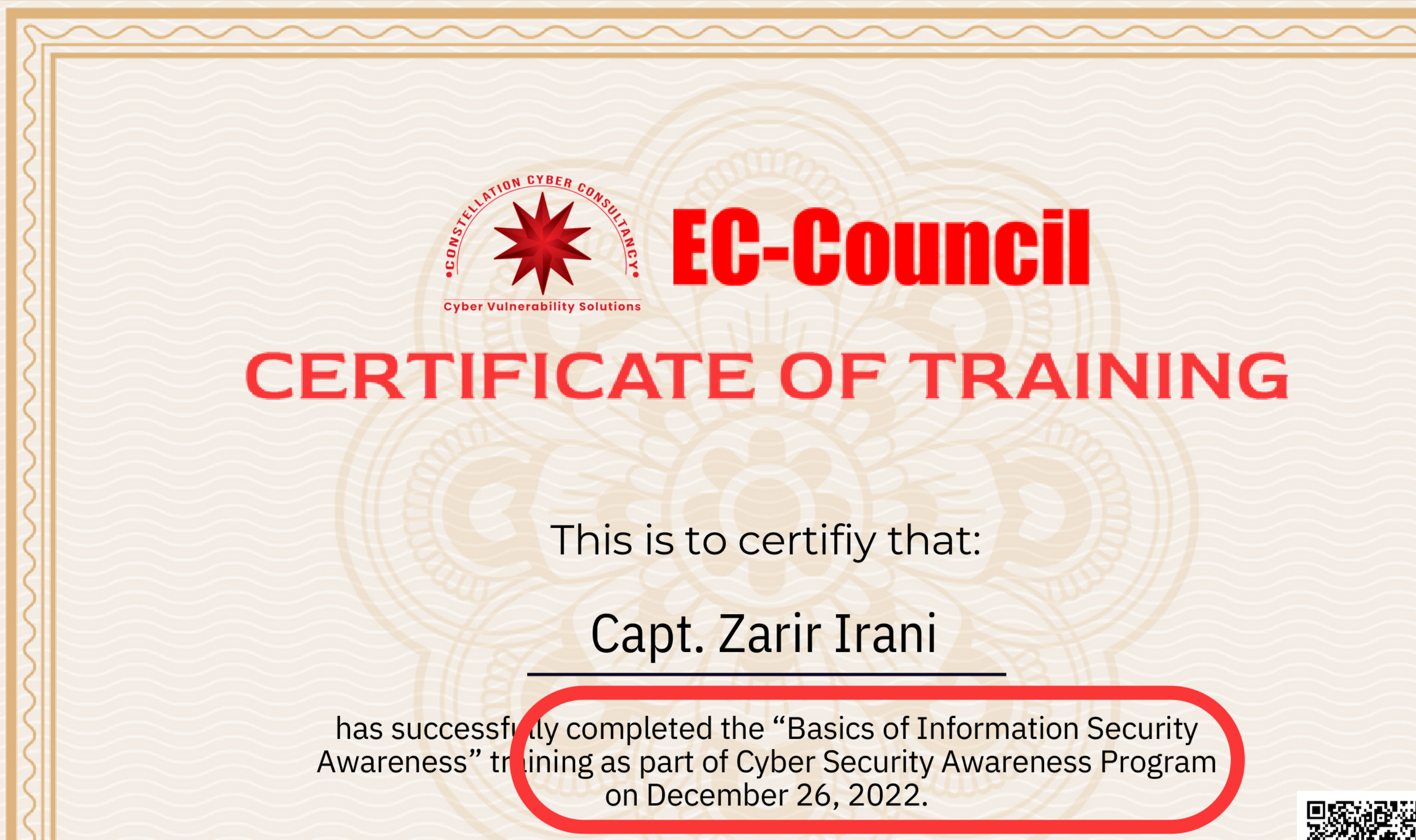
CERTIFICATE OF TRAINING

This is to certifiy that:

Capt. Zarir Irani

has successfully completed the “Smishing” training as part of Cyber Security Awareness Program on January 16, 2023.

Certificate Number: 16738-52717-765



CONSTELLATION CYBER CONSULTANCY

Cyber Vulnerability Solutions

EC-Council

CERTIFICATE OF TRAINING

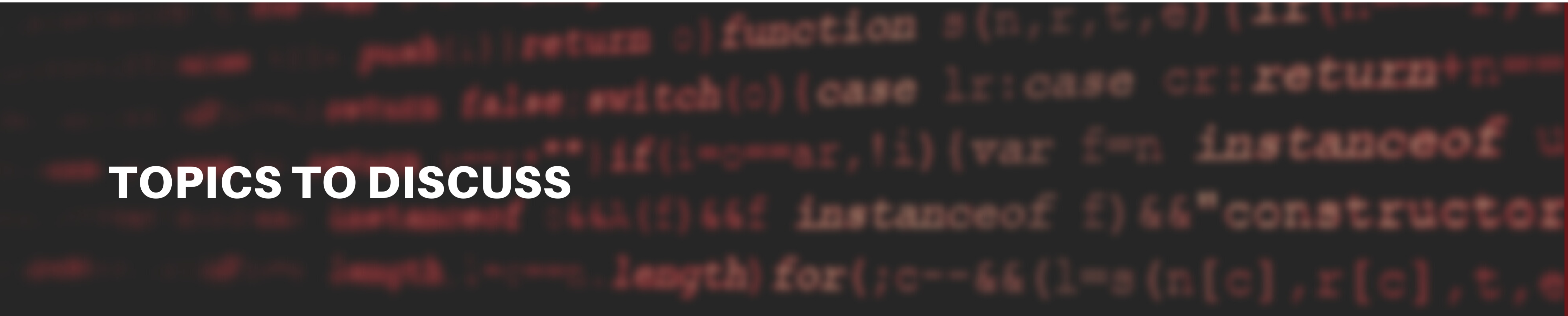
This is to certifiy that:

Capt. Zarir Irani

has successfully completed the “Basics of Information Security Awareness” training as part of Cyber Security Awareness Program on December 26, 2022.

Agenda

- The types of digital risks your organization is exposed to.
- A deep dive into the **Dark Web** to understand what's for sale.
- How to **mitigate** the risks of Cyber Attack
- Differentiating between an independent and in-house assessment.

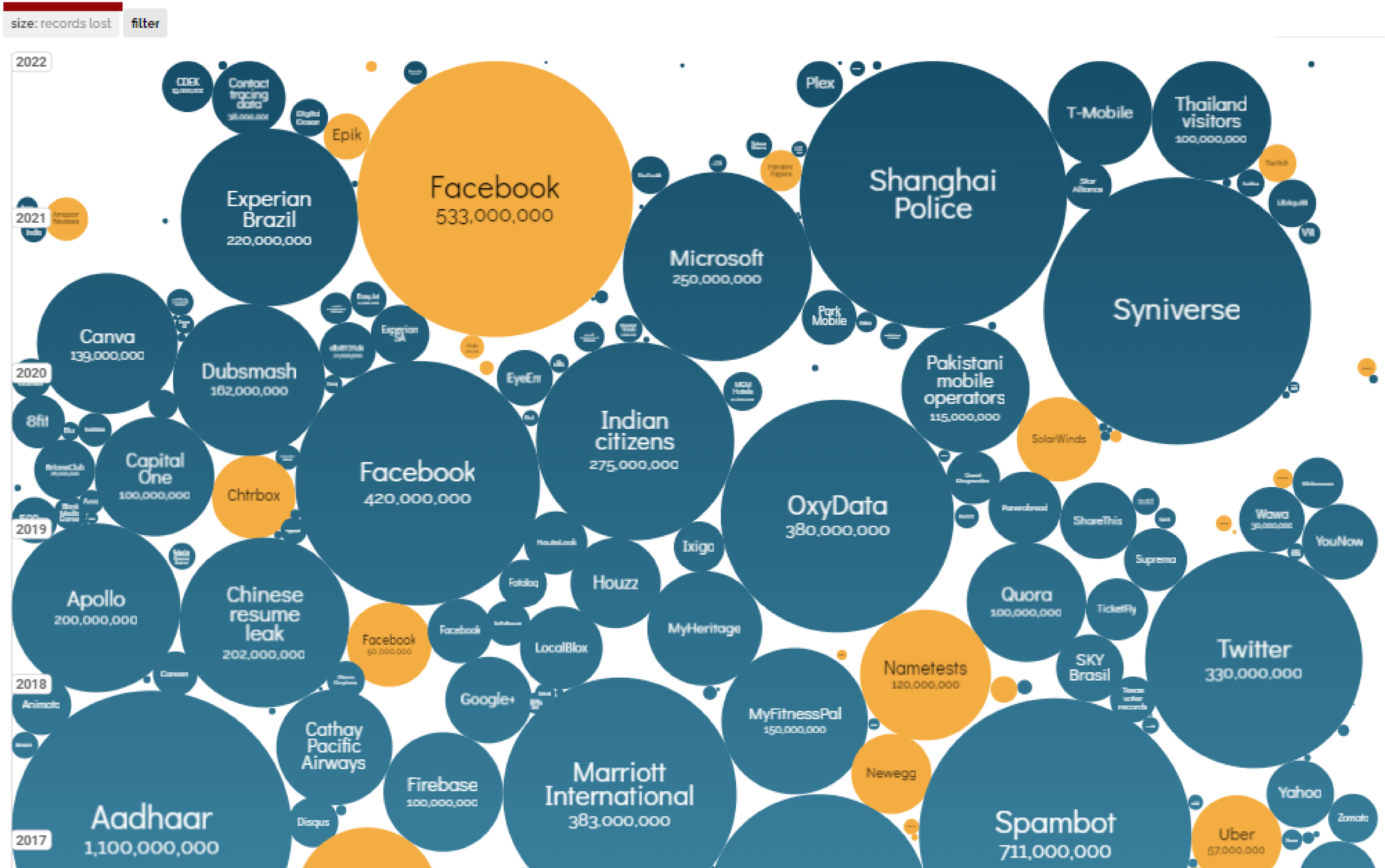


TOPICS TO DISCUSS

World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Sep 2022



THECYBERCONSULTANCY.COM

Reference

World's Biggest Data Breaches & Hacks — Information is Beautiful

source: New York Times, Forbes, The Guardian, Tech Radar, BBC, PC Mag, Tech Crunch & others

Cyber Vulnerability Solutions

Digital Risks

The Dangerous Types

Cybersecurity Risk

Cyber Attacks that can bring a halt to the normalcy of any business.

Data Privacy Risk

Critical business data are prone to being misused for personal gains.

Compliance Risk

Poor practice of regulations can attract heavy fines and penalties.

Reputation Risk

Damage to reputation of business caused by Cyber Attacks.

Third Party Risk

External vendor can bring vulnerabilities to your infrastructure.

Human Error Risk

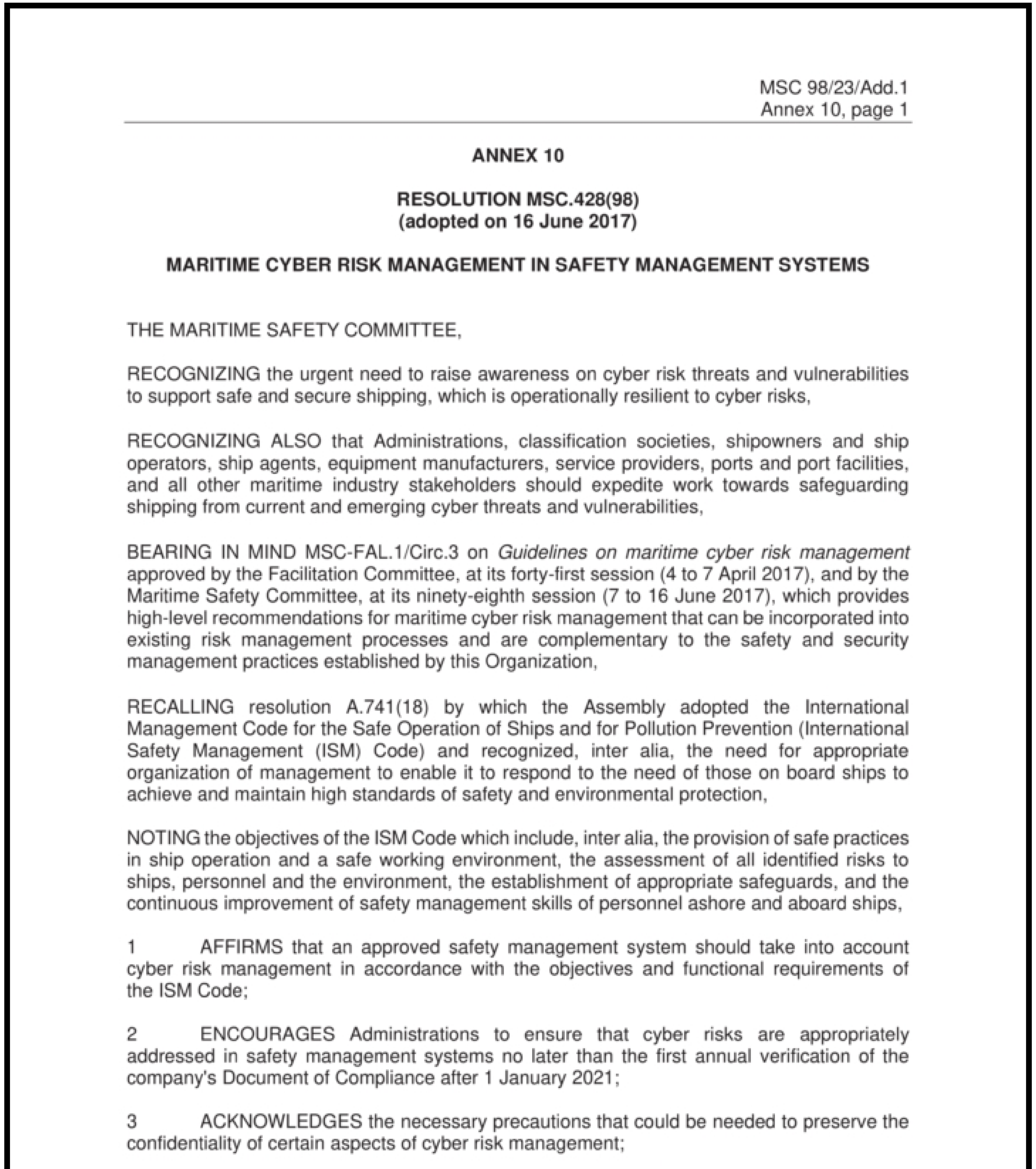
Unintentional action by employees that causes a security breach.

HOW COMPANIES PUT THEIR REPUTATION AT RISK

- Insecure practices make applications vulnerable, resulting in data breaches.
- Phishing scams lead to a loss of trust among companies.
- Using offensive messages to affect stakeholders' reputations

THIRD-PARTY SYSTEMS ONBOARD NEED ATTENTION

- Third-party with permission to store or access your business data.
- Insecure third-party systems causes violations and fines
- Disruption of ships's operation caused by third-party systems.



ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

Link for full document

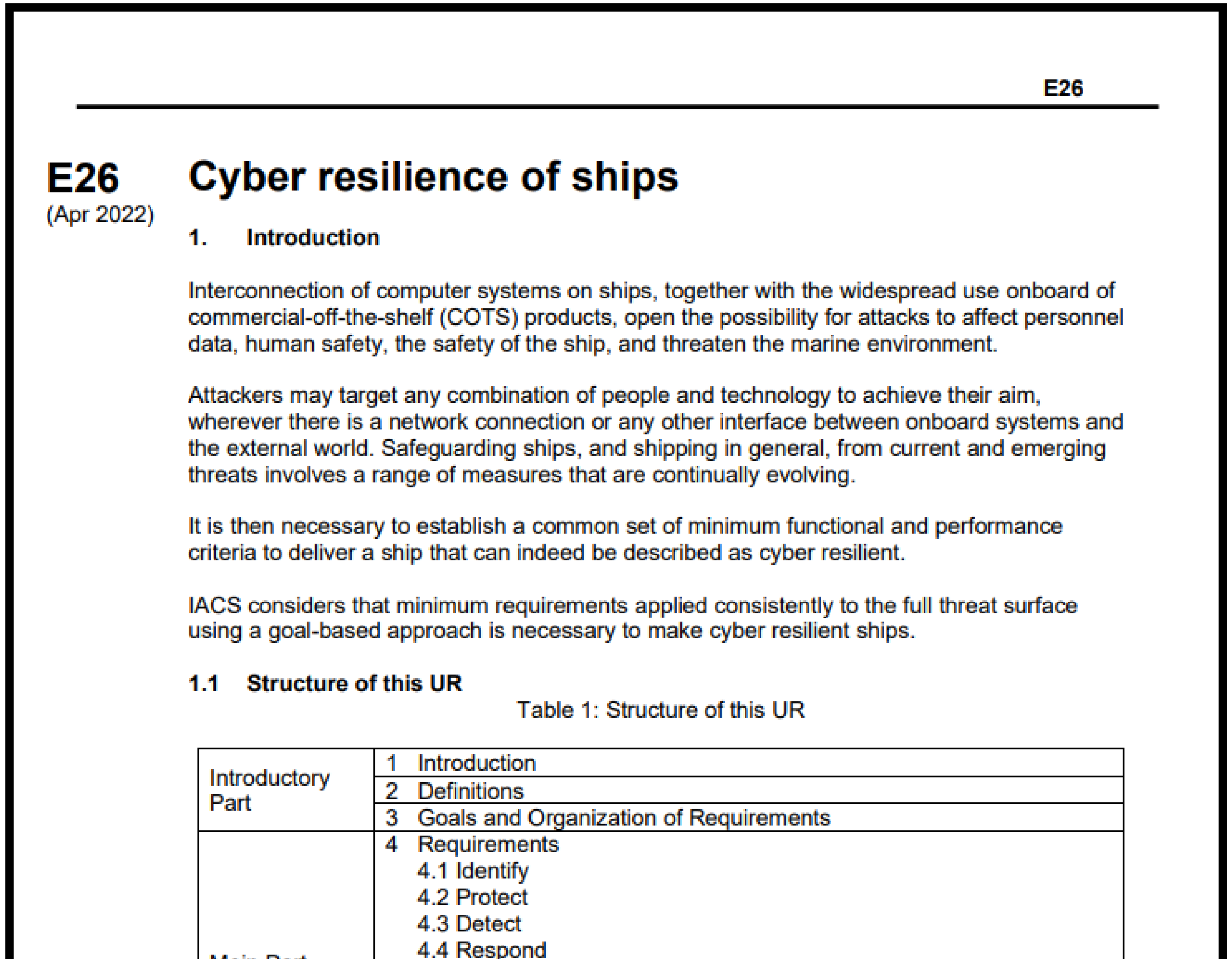
INTERNATIONAL
MARITIME
ORGANIZATION

IMO Resolution MSC.428(98)

IACS International Association of Classification Societies

Scan to download

UR E26 Cyber resilience of ships
New Resolution to apply on April 2022



E26 Cyber resilience of ships

(Apr 2022)

1. Introduction

Interconnection of computer systems on ships, together with the widespread use onboard of commercial-off-the-shelf (COTS) products, open the possibility for attacks to affect personnel data, human safety, the safety of the ship, and threaten the marine environment.

Attackers may target any combination of people and technology to achieve their aim, wherever there is a network connection or any other interface between onboard systems and the external world. Safeguarding ships, and shipping in general, from current and emerging threats involves a range of measures that are continually evolving.

It is then necessary to establish a common set of minimum functional and performance criteria to deliver a ship that can indeed be described as cyber resilient.

IACS considers that minimum requirements applied consistently to the full threat surface using a goal-based approach is necessary to make cyber resilient ships.

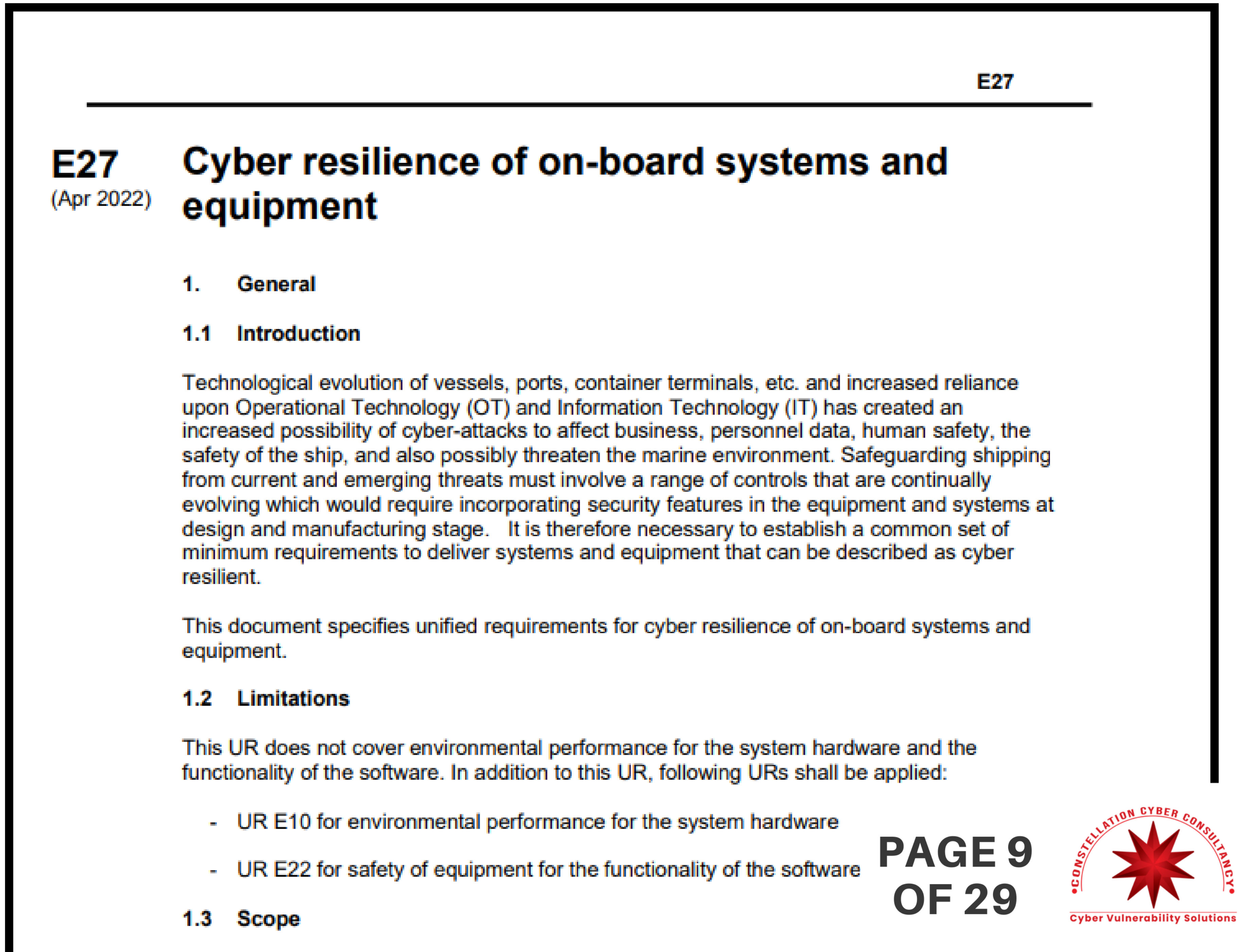
1.1 Structure of this UR

Table 1: Structure of this UR

Introductory Part	1 Introduction
	2 Definitions
	3 Goals and Organization of Requirements
Main Part	4 Requirements 4.1 Identify 4.2 Protect 4.3 Detect 4.4 Respond

Scan to download

UR E27 Cyber resilience of on-board systems.
New Resolution to apply on April 2022



E27 Cyber resilience of on-board systems and equipment

(Apr 2022)

1. General

1.1 Introduction

Technological evolution of vessels, ports, container terminals, etc. and increased reliance upon Operational Technology (OT) and Information Technology (IT) has created an increased possibility of cyber-attacks to affect business, personnel data, human safety, the safety of the ship, and also possibly threaten the marine environment. Safeguarding shipping from current and emerging threats must involve a range of controls that are continually evolving which would require incorporating security features in the equipment and systems at design and manufacturing stage. It is therefore necessary to establish a common set of minimum requirements to deliver systems and equipment that can be described as cyber resilient.

This document specifies unified requirements for cyber resilience of on-board systems and equipment.

1.2 Limitations

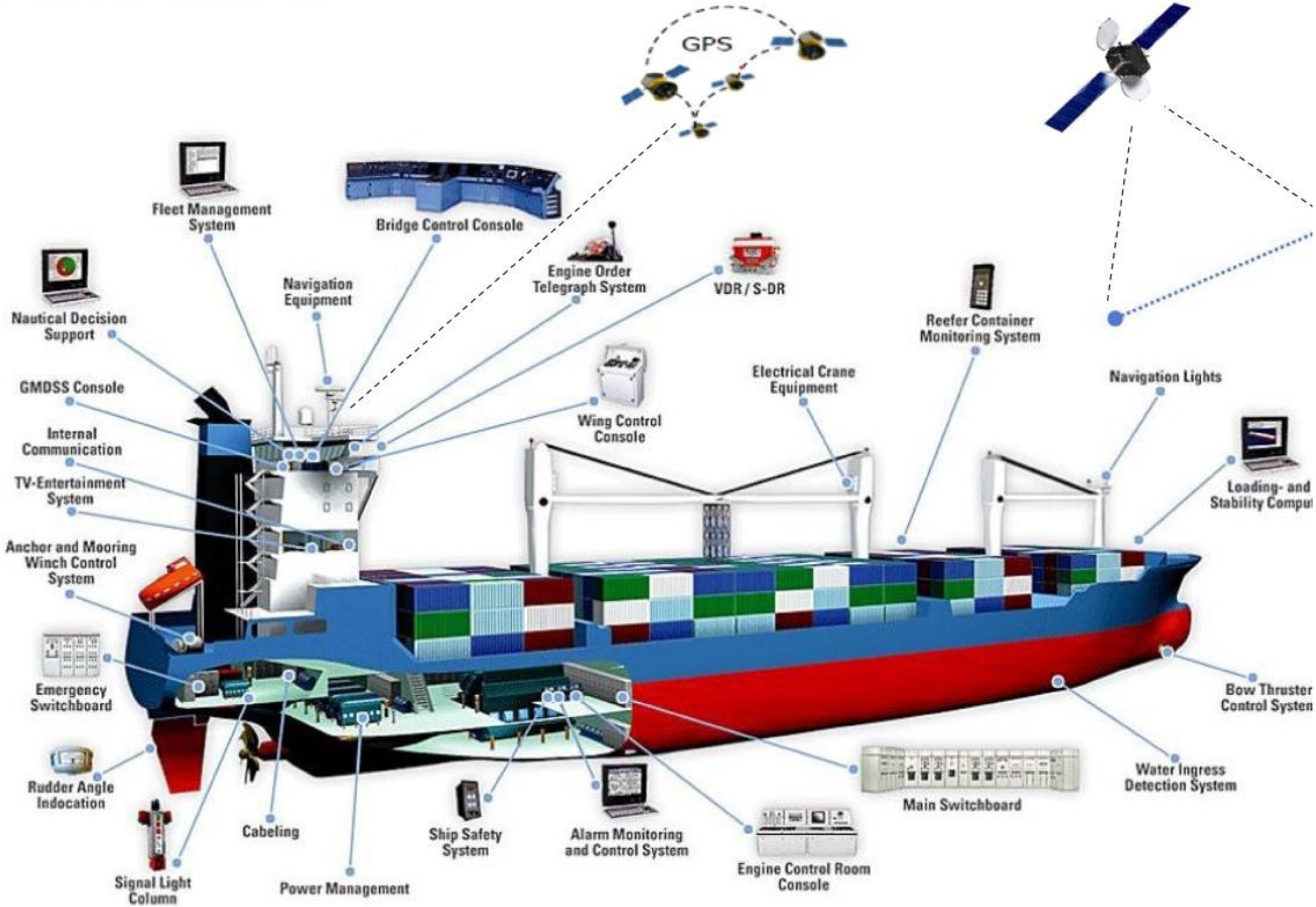
This UR does not cover environmental performance for the system hardware and the functionality of the software. In addition to this UR, following URs shall be applied:

- UR E10 for environmental performance for the system hardware
- UR E22 for safety of equipment for the functionality of the software

1.3 Scope

AN INCREASINGLY DIGITISED SHIP

IT & OT SYSTEMS ONBOARD

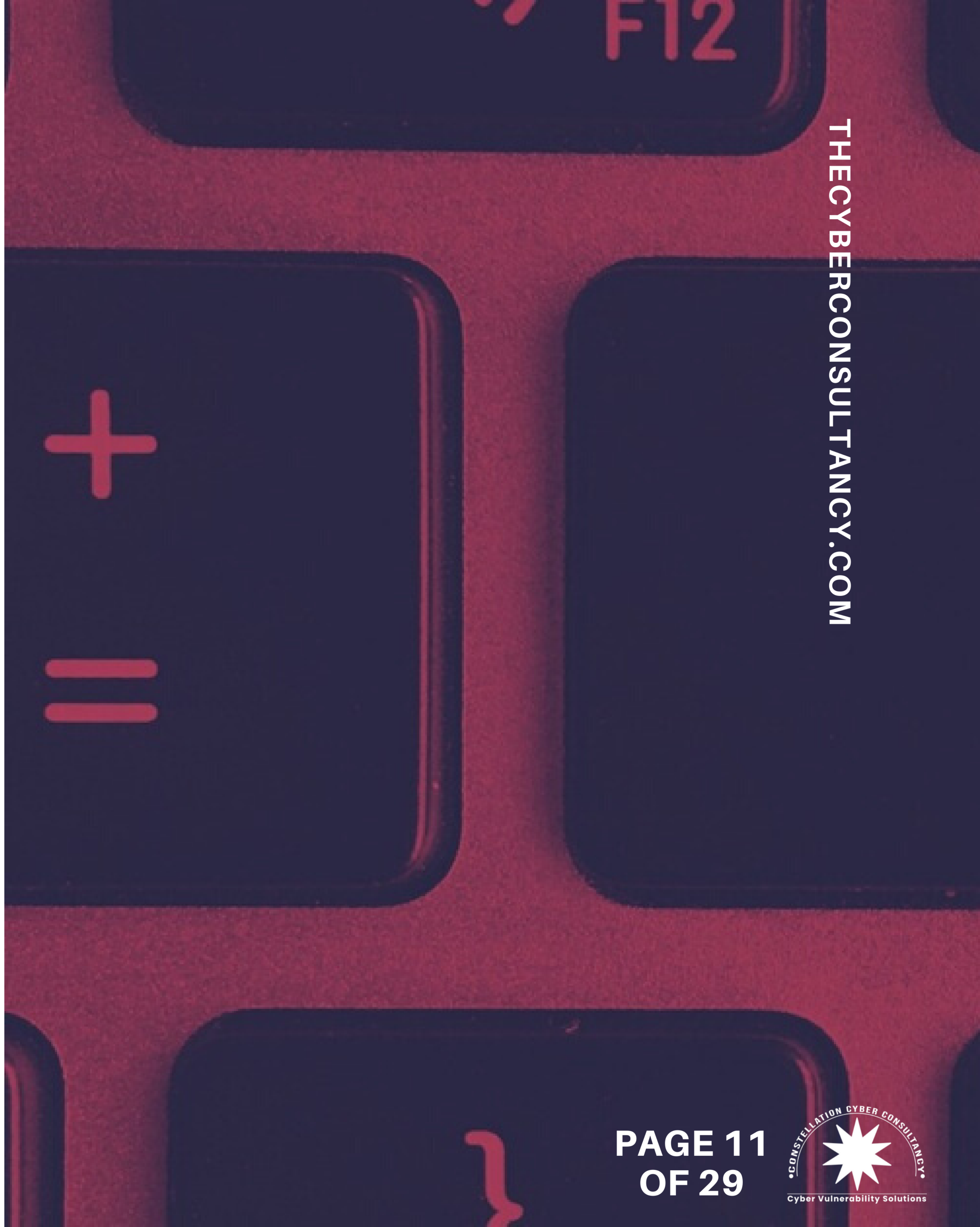

GPS
Fleet Management System
Bridge Control Console
Navigation Equipment
Nautical Decision Support
Engine Order Telegraph System
VDR / S-DR
GMDSS Console
Reefer Container Monitoring System
Electrical Crane Equipment
Navigation Lights
Wing Control Console
Internal Communication
TV-Entertainment System
Loading- and Stability Comput
Anchor and Mooring Winch Control System
Emergency Switchboard
Bow Thruster Control Systen
Water Ingress Detection System
Main Switchboard
Rudder Angle Indocation
Cabeling
Ship Safety System
Alarm Monitoring and Control System
Engine Control Room Console
Signal Light Column
Power Management

THECYBERCONSULTANCY.COM

Third Party Risk

Third-party risk is the likelihood that your business might experience a data breach or reputational damage when you outsource particular services or use software made by third parties to carry out specified duties.

80% of Organizations experienced a data breach from a Third Party


F12
THECYBERCONSULTANCY.COM
CONSTELLATION CYBER CONSULTANCY
Cyber Vulnerability Solutions

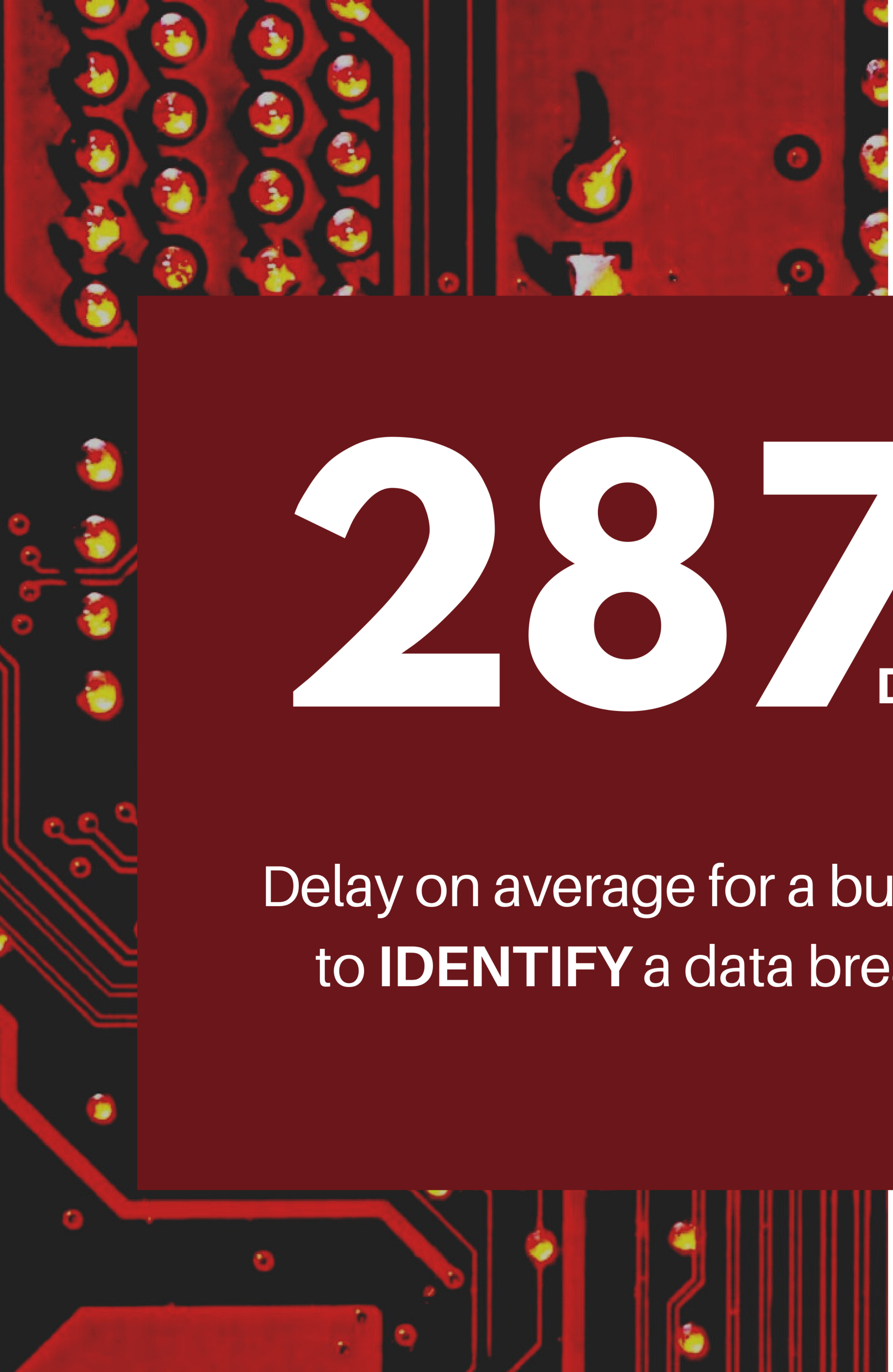
Risk due to Human Error

Human error is one of the biggest security threats that organisations face.

Concerns on board ships by human error can lead to various problems that impact the safety of the crew and vessel.

Human Error is responsible for 82% of Cybersecurity Breaches

THECYBERCONSULTANCY.COM



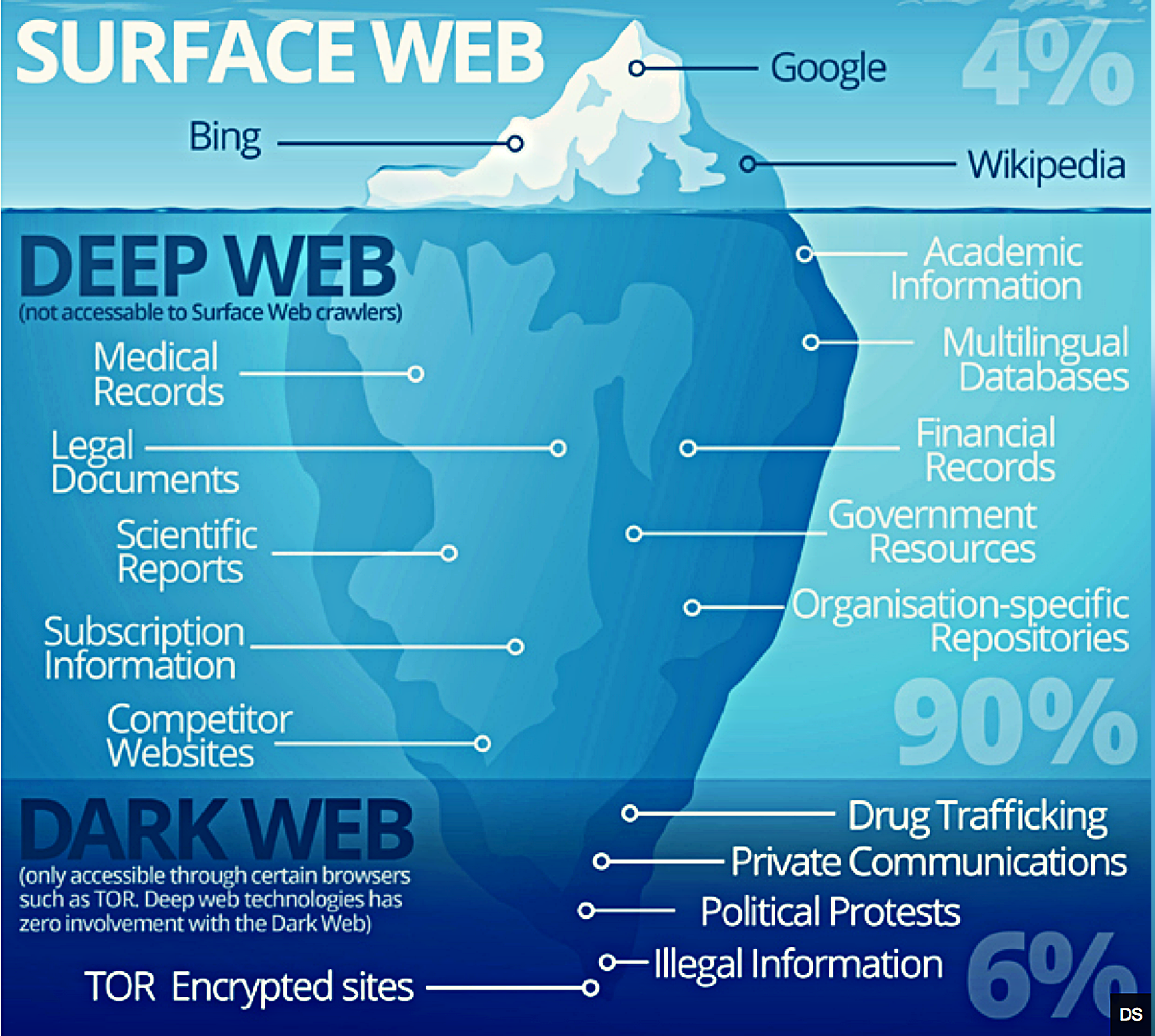
287 DAYS

Delay on average for a business to **IDENTIFY** a data breach.

80 DAYS

Average days for a business to **CONTAIN** a data breach.

Reference
IBM Data Breach Report 2022



SURFACE WEB

Google

Bing

Wikipedia

4%

DEEP WEB

(not accessable to Surface Web crawlers)

Medical Records

Legal Documents

Scientific Reports

Subscription Information

Competitor Websites

Academic Information

Multilingual Databases

Financial Records

Government Resources

Organisation-specific Repositories

90%

DARK WEB

(only accessible through certain browsers such as TOR. Deep web technologies has zero involvement with the Dark Web)

TOR Encrypted sites

Drug Trafficking

Private Communications

Political Protests

Illegal Information

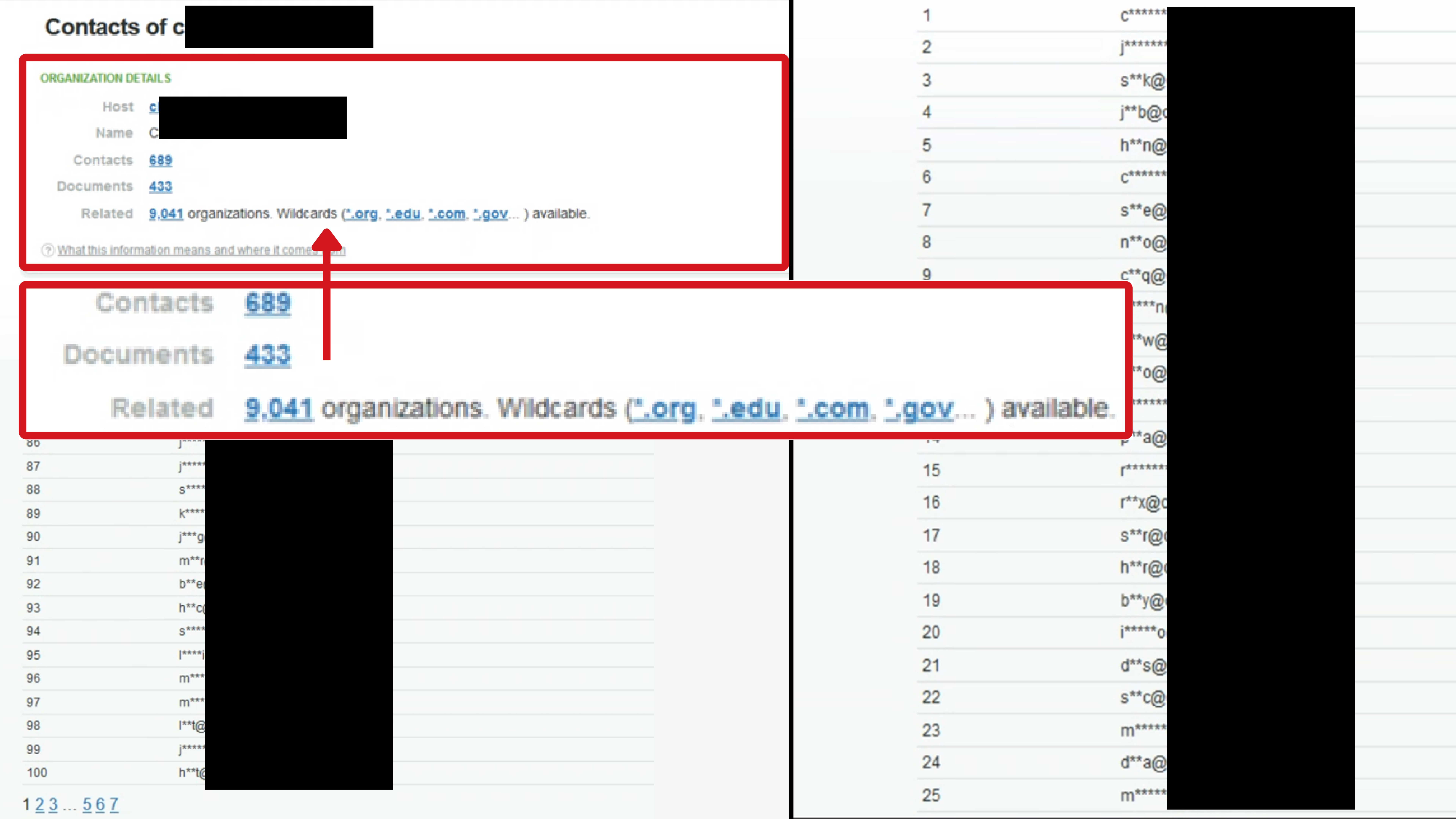
6%

WHERE IS YOUR DATA?

Live Demonstration

IS YOUR DATA STOLEN?

PROBING THE DARK WEB



Contacts of c[redacted]

ORGANIZATION DETAILS

Host	c[redacted]
Name	C[redacted]
Contacts	689
Documents	433
Related	9,041 organizations. Wildcards (*.org, *.edu, *.com, *.gov...) available.

What this information means and where it comes from

Contacts 689

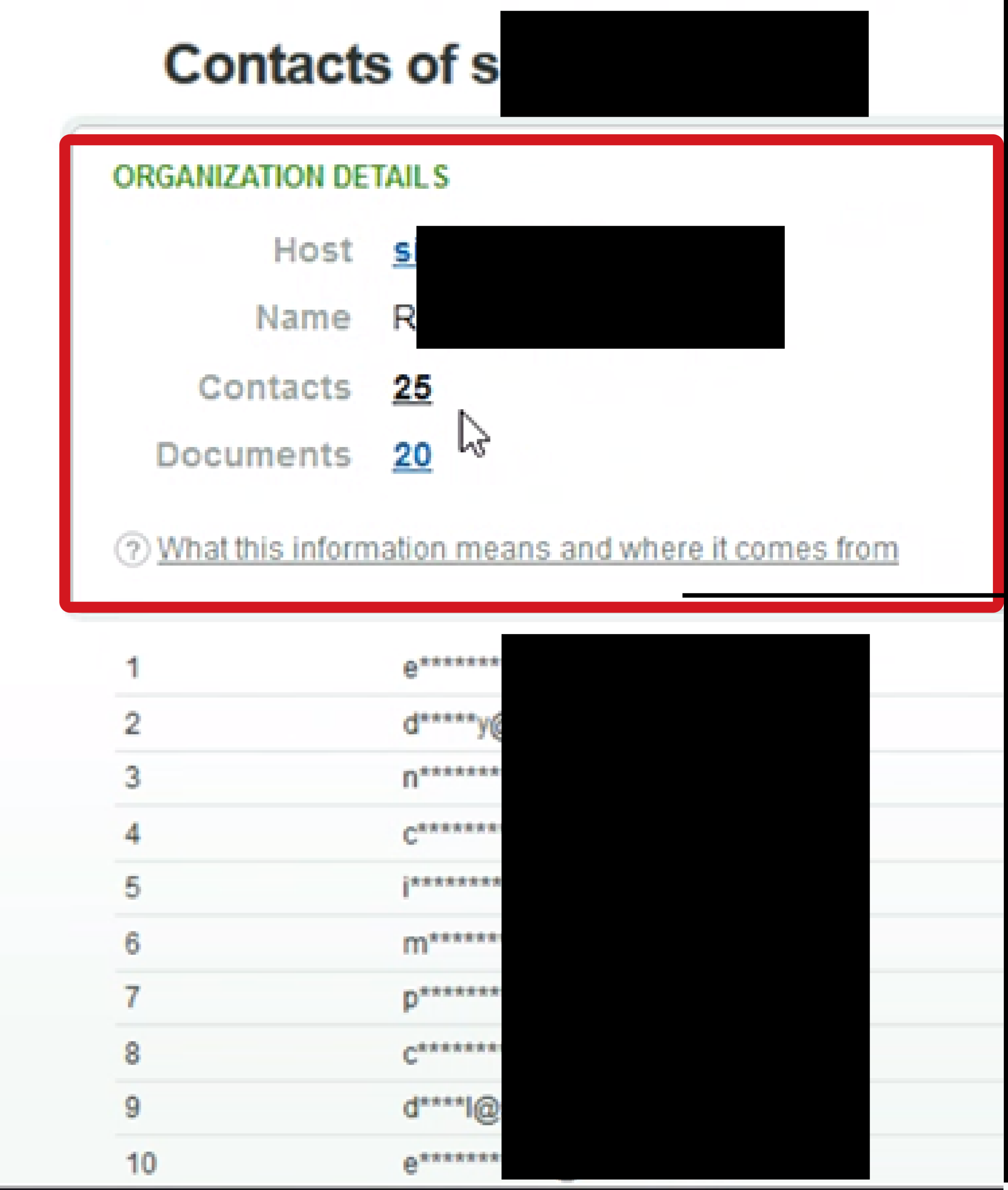
Documents 433

Related 9,041 organizations. Wildcards (*.org, *.edu, *.com, *.gov...) available.

86	j****[redacted]
87	j****[redacted]
88	s****[redacted]
89	k****[redacted]
90	j***g[redacted]
91	m**r[redacted]
92	b**e[redacted]
93	h**c[redacted]
94	s****[redacted]
95	l****i[redacted]
96	m***[redacted]
97	m***[redacted]
98	l**t@[redacted]
99	j*****[redacted]
100	h**t@[redacted]

1 2 3 ... 5 6 7

1	c******[redacted]
2	j******[redacted]
3	s**k@[redacted]
4	j**b@[redacted]
5	h**n@[redacted]
6	c******[redacted]
7	s**e@[redacted]
8	n**o@[redacted]
9	c**q@[redacted]
	***n[redacted]
	**w@[redacted]
	**o@[redacted]
	******[redacted]
	p**a@[redacted]
15	r******[redacted]
16	r**x@[redacted]
17	s**r@[redacted]
18	h**r@[redacted]
19	b**y@[redacted]
20	i*****o[redacted]
21	d**s@[redacted]
22	s**c@[redacted]
23	m*****[redacted]
24	d**a@[redacted]
25	m*****[redacted]



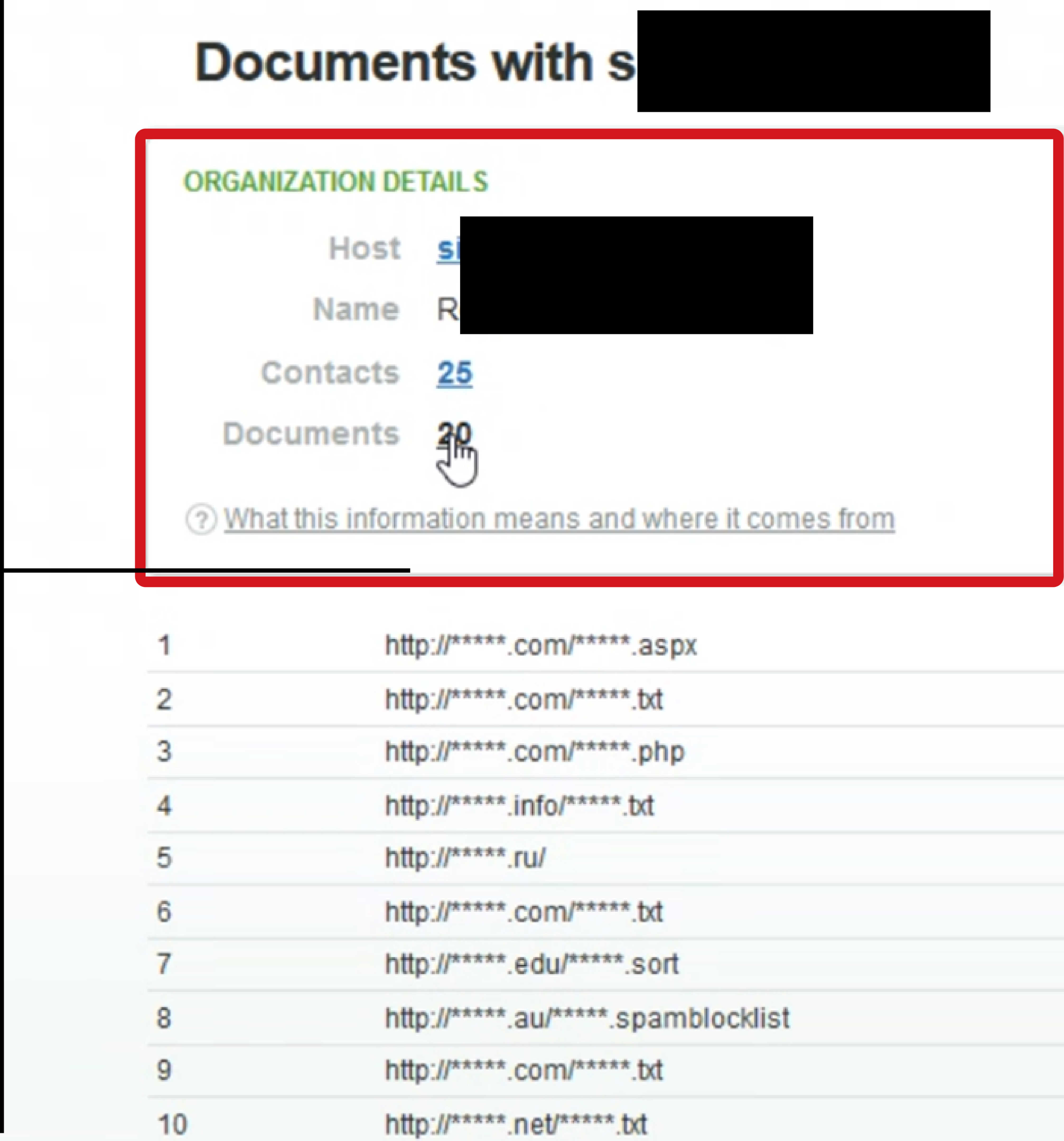
Contacts of s[redacted]

ORGANIZATION DETAILS

Host	si[redacted]
Name	R[redacted]
Contacts	25
Documents	20

ⓘ What this information means and where it comes from

1	e*******[redacted]
2	d*****y@[redacted]
3	n*******[redacted]
4	c*******[redacted]
5	i*******[redacted]
6	m*******[redacted]
7	p*******[redacted]
8	c*******[redacted]
9	d****l@[redacted]
10	e*******[redacted]



Documents with s[redacted]

ORGANIZATION DETAILS

Host	si[redacted]
Name	R[redacted]
Contacts	25
Documents	20

ⓘ What this information means and where it comes from

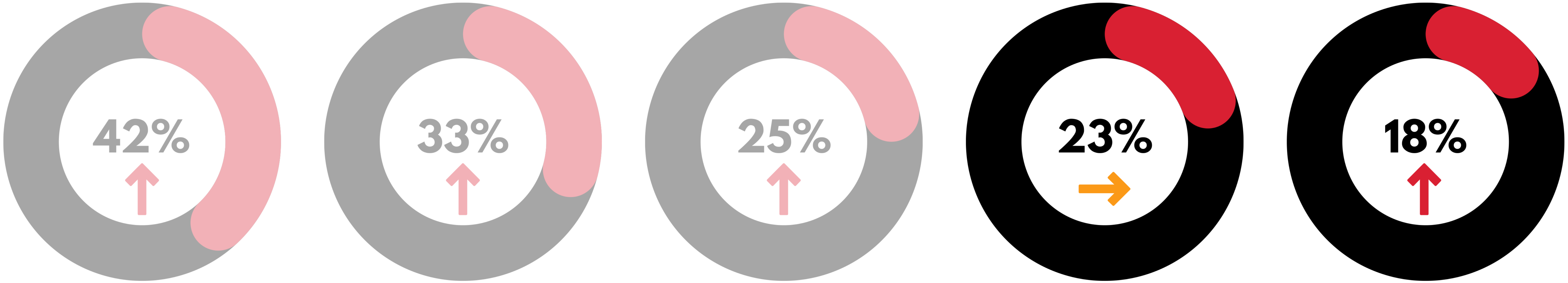
1	http://*****.com/*****.aspx
2	http://*****.com/*****.txt
3	http://*****.com/*****.php
4	http://*****.info/*****.txt
5	http://*****.ru/
6	http://*****.com/*****.txt
7	http://*****.edu/*****.sort
8	http://*****.au/*****.spamblocklist
9	http://*****.com/*****.txt
10	http://*****.net/*****.txt

Recent Known Attacks on Maritime and Offshore

S.NO	COMPANY NAME	TYPE OF ATTACK	YEAR	DESCRIPTION
1	S.A.	Data Breach	2021	Employees personnel information like scanned copy of passport, etc. were stolen.
2	R.D.	Clop Ransomware	2021-2022	A file-transfer application had been compromised.
3	M.M.	NotPetya Ransomware	2017	Attackers spread the malware after seizing control of the software update mechanism.
4	C.C.	Ransomware	2020	Encrypt the company's system – which included its booking facility.
5	D.L.	Phisihing Attack	2022	Phishing attack

Top 5 Risks

Marine and Shipping



Business Interruption (including supply chain disruption)

Natural catastrophes (storm, earthquake, weather events)

Fire and explosion

Cyber incidents (data breach, IT failures, cyber crime)

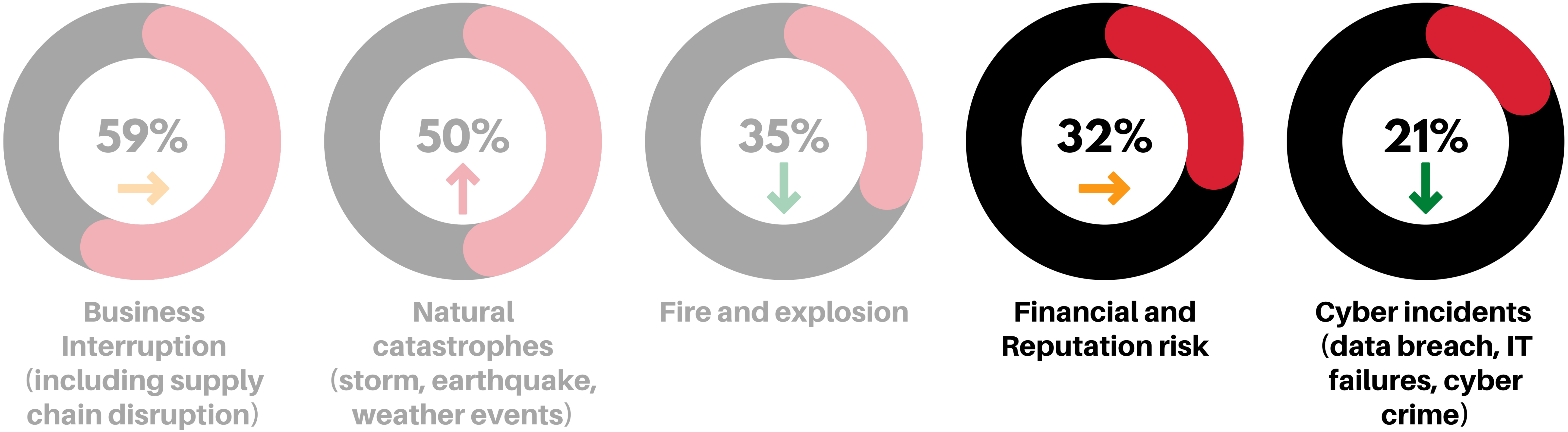
Financial and Reputation risk

Allianz Global Corporate and Speciality

Figures represent how often a risk was selected as a percentage of all responses for that industry sector

Top 5 Risks

Oil and Gas

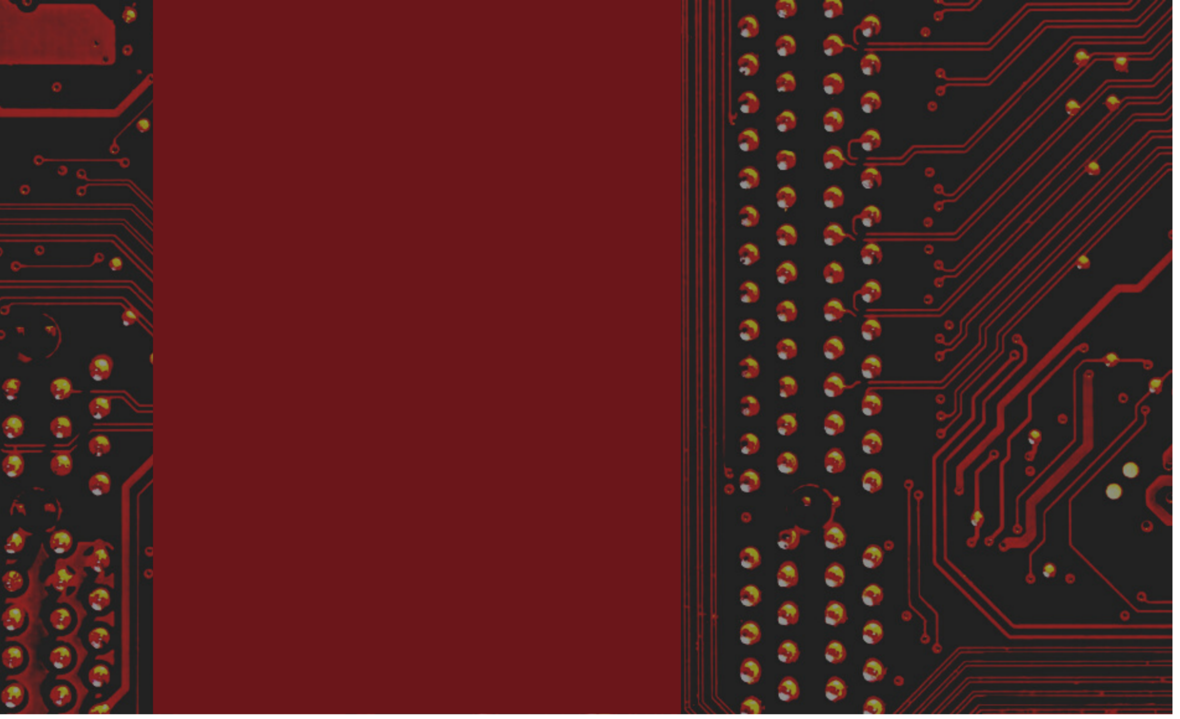


Allianz Global Corporate and Speciality

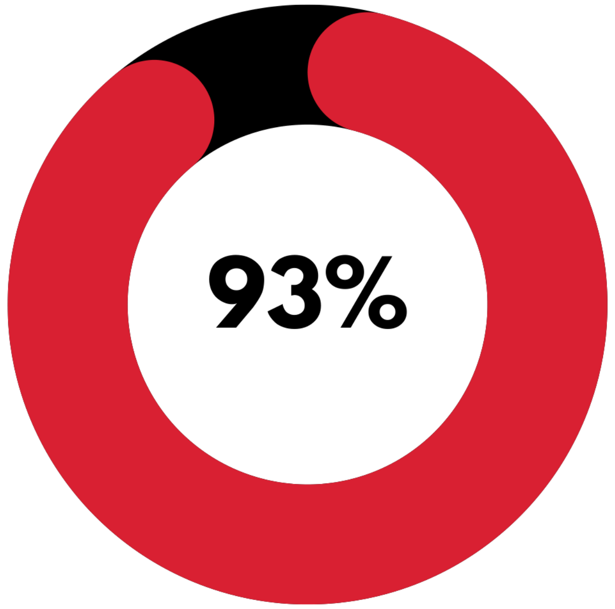
Figures represent how often a risk was selected as a percentage of all responses for that industry sector

Stolen Data Available on the Dark Web

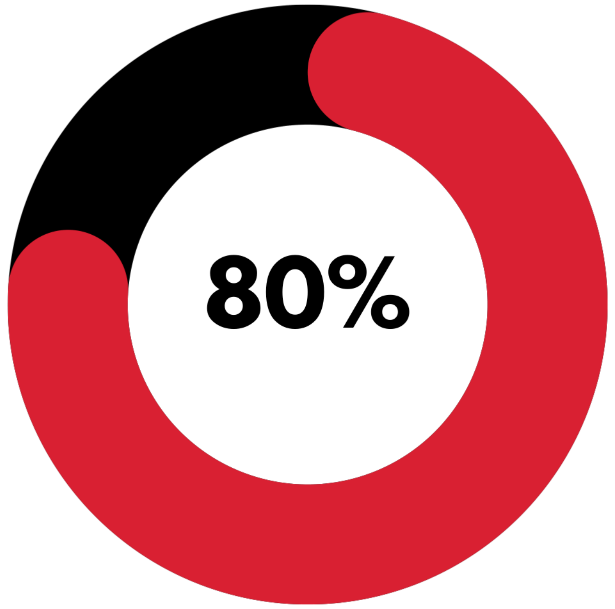
COMPANY	DARK WEB LINKS
S.A.	[redacted]d2xrppj63srydgjg4cf2id.onion/email/sa[redacted]tml
R.D.	[redacted]zaeax3hwhidbqkjzva3223jpxqd.onion/sp[redacted]cts/
I.C.	[redacted]4m4dkburo73pzuqfdumcntqdokyd.onion/articles/article-134.html
H.L.	[redacted]h53jzrx7ipcrbjz5b2ad.onion/bd1029b05168289713d7247cc77006320a56a45/



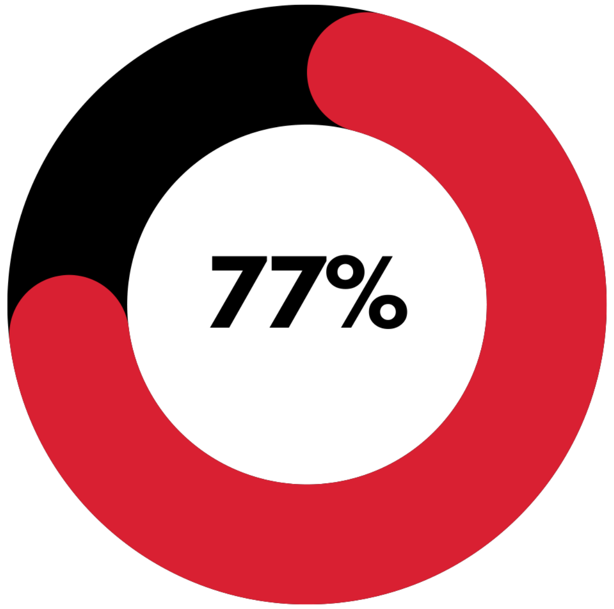
Eye-opening Cybersecurity Statistics



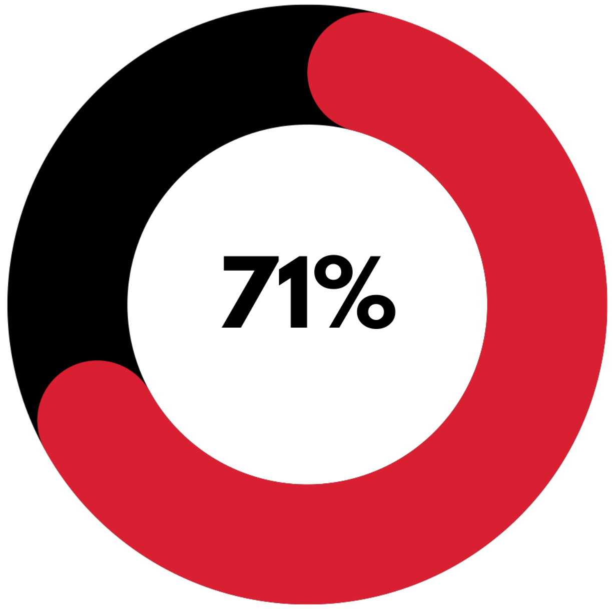
Organisations affected by Talent Shortage for Cybersecurity



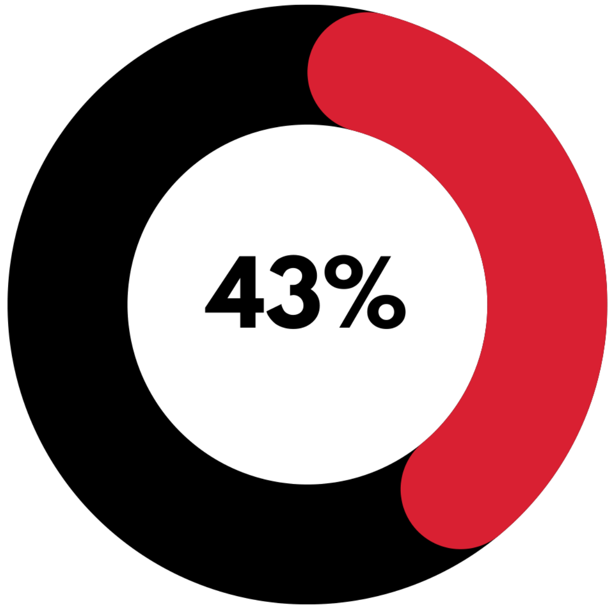
Organized crime responsible for all security breaches.



Companies **DO NOT** have Incident Response Plan.



Organizations worldwide have been victims of Ransomware



Small and Medium business affected by Cyberattacks.

THECYBERCONSULTANCY.COM

Ways to Reduce Cybersecurity Risk for Your Organization

Encrypt Your Data and Create **Backups**

Conduct Regular Employee **Training**

Keep Your System and Software **Updated**

Use Strong and Unique **Passwords**

Assess and **Monitor** Your Vendors

Pay Close Attention to **Physical Security**

Put a **Killswitch** in Place

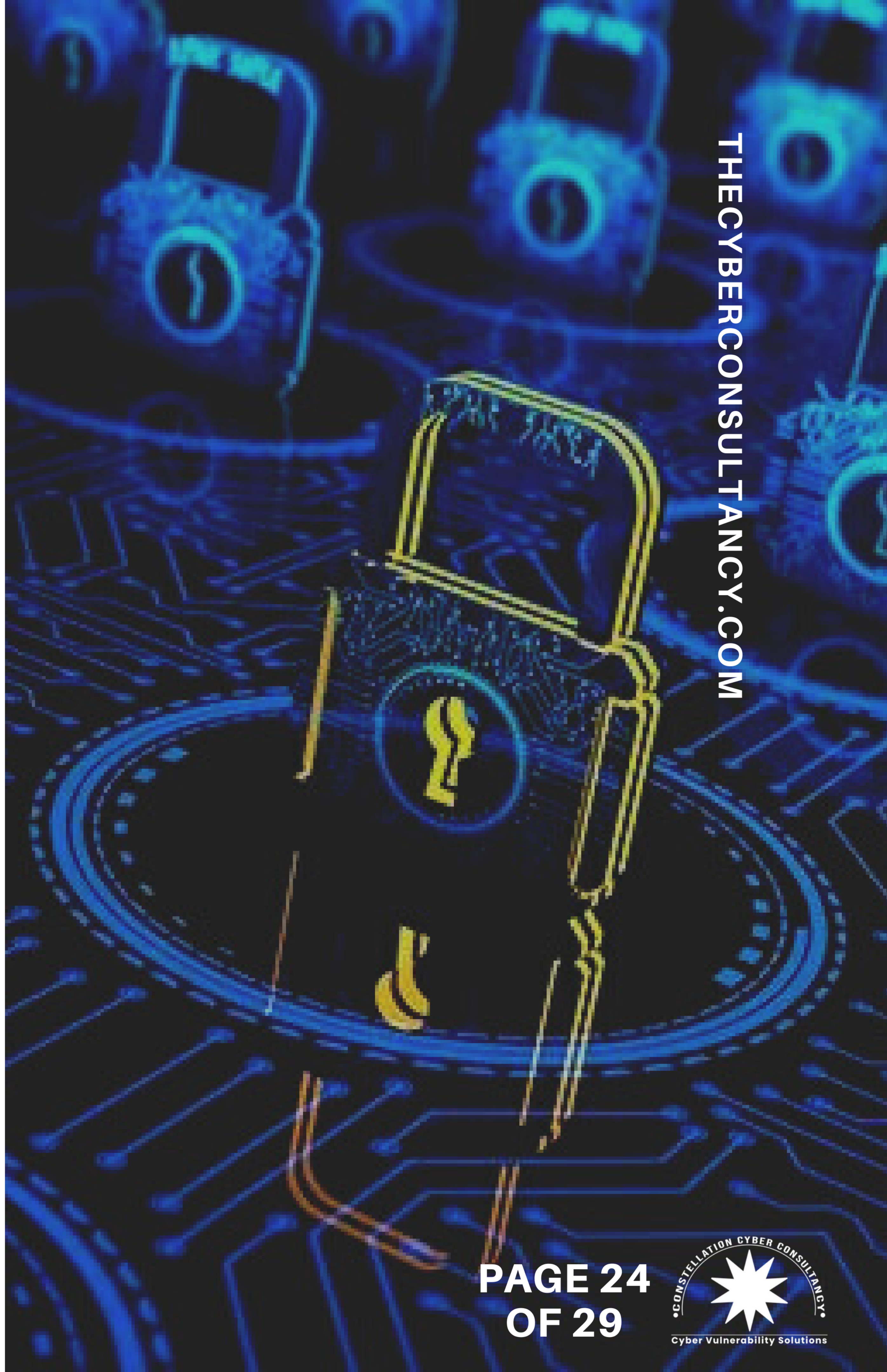
Choose the Right **Firewalls**

Reduce Your **Attack Surface**

Create A Secure Cybersecurity **Policy**

Immediate Steps to Lower Risk to Cyber Attacks

- Developing a Vulnerability Management Program
- Conduct routine Penetration Testing
- Implementing Security Information and Event Management (SIEM)
- Keep your systems software up-to-date
- Establish cybersecurity policies with Business Partners
- Make sure data is backed-up to protect from downtime and data loss



THECYBERCONSULTANCY.COM

CONSTELLATION CYBER CONSULTANCY
Cyber Vulnerability Solutions

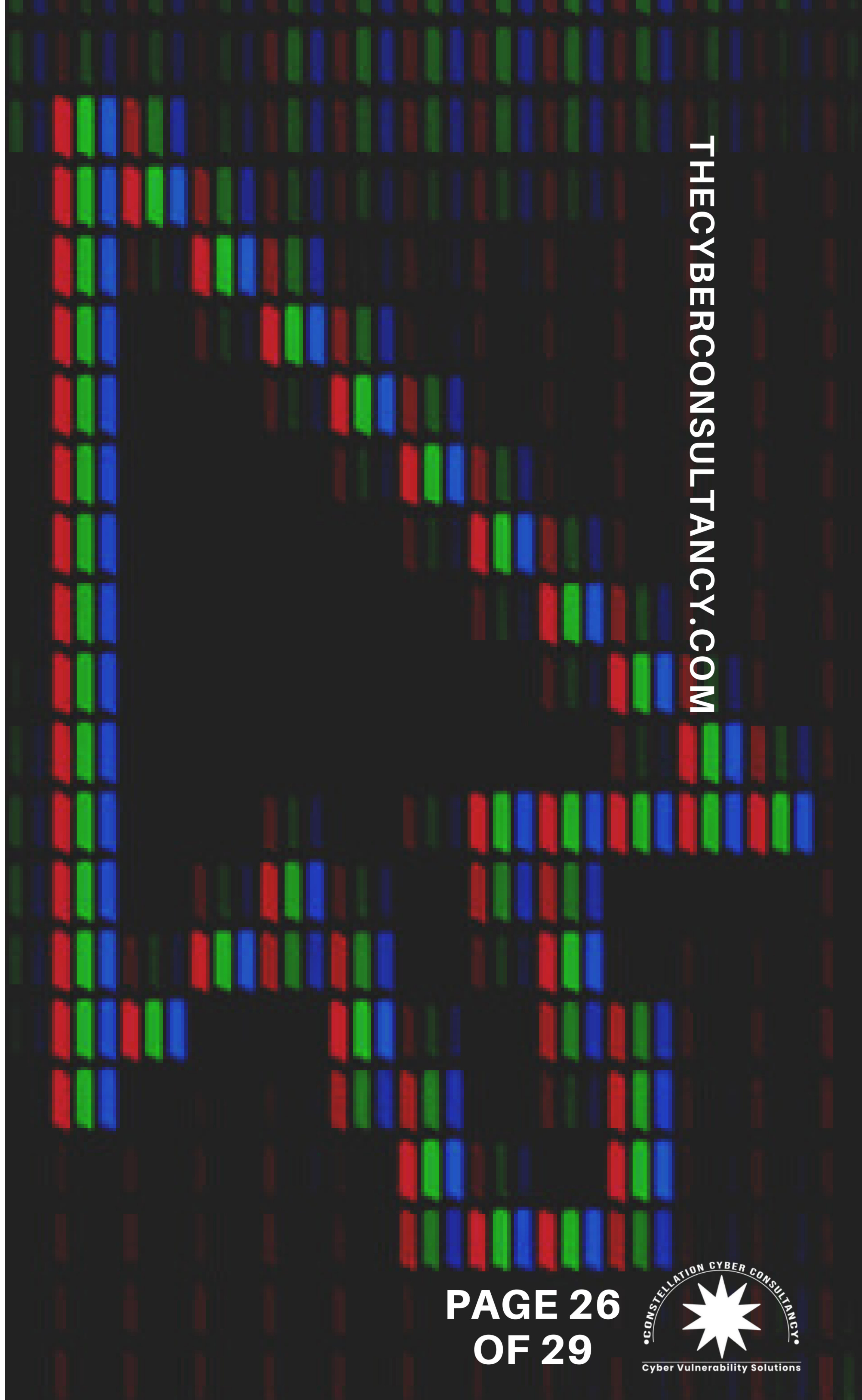
CONSTELLATION CYBER CONSULTANCY

Cyber Vulnerability Solutions

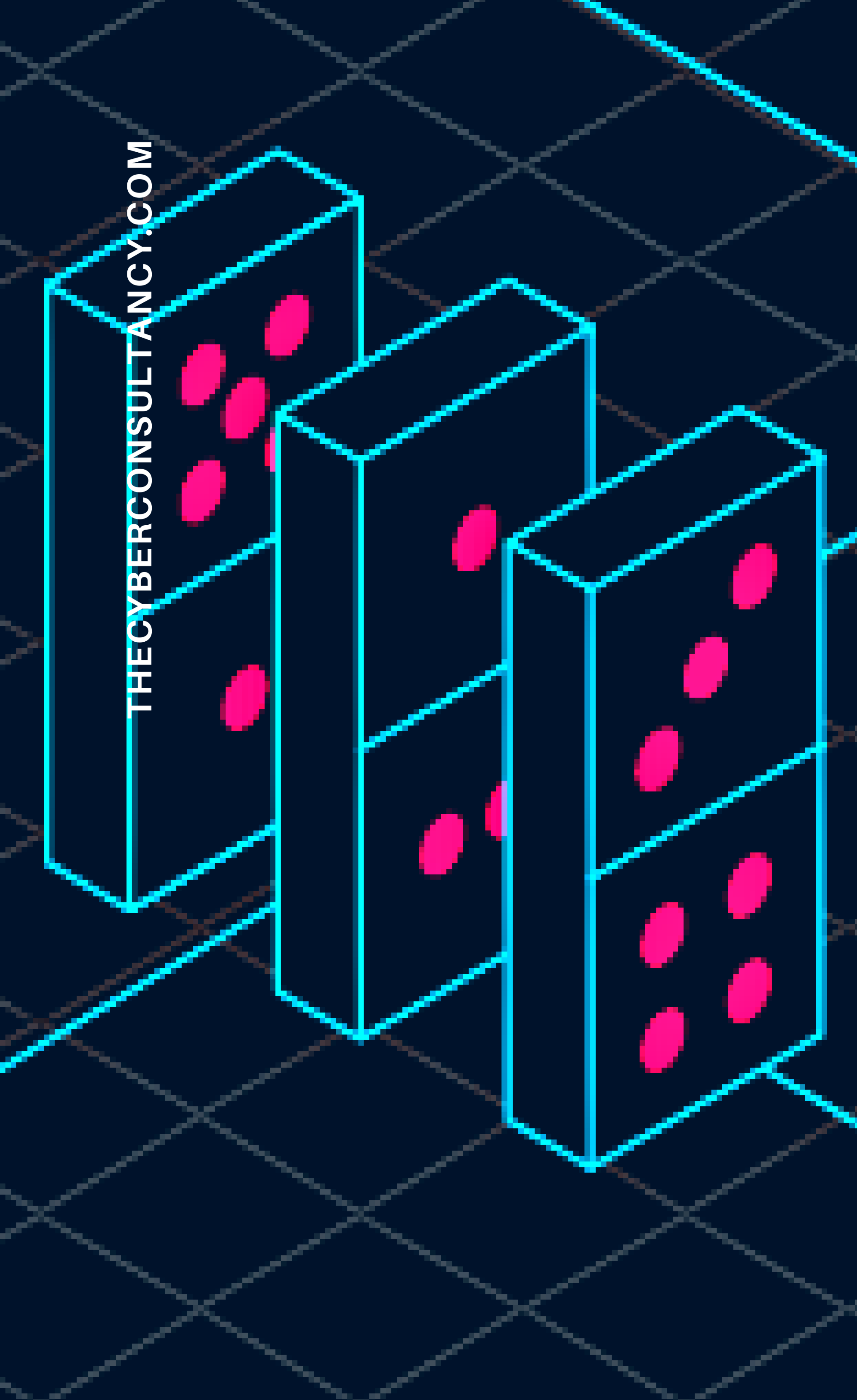
How can we help you?

Our Cyber Security Services.

- Provide consultation to our clients to help protect, design and implement a cyber secure environment.
- Adopting the industrial standard for Cybersecurity Requirements with IMO Resolution MSC.428(98)
- Helps clients to identify potential risks and provide mitigation and recommendation to minimize the attack surface which helps to improve your infrastructure.
- Provide comprehensive awareness campaign to onboard personnel to keep aware of new threats and risks.



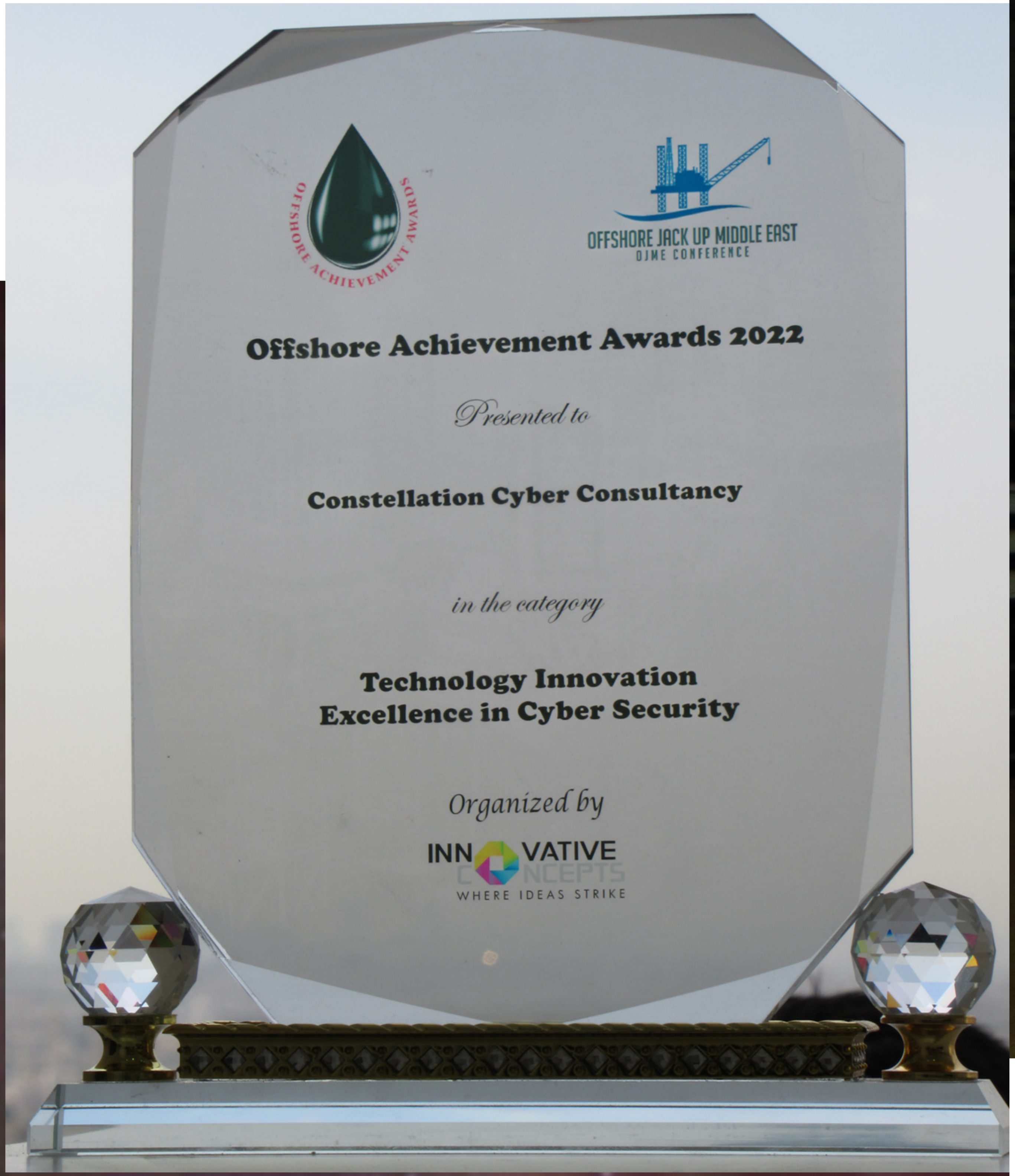
THECYBERCONSULTANCY.COM



Our Experience and Professional Expertise.

- Design a secure network infrastructure and help in deployment and documentation that includes firewall, filtering and traffic logging for analysis.
- Configure User right privileges (access to confidential information between crews)
- Training staff on potential cyber risks and to be aware of plausible cyber negligence behaviour.

Offshore Achievement Awards 2022



Offshore Achievement Awards 2022

Presented to

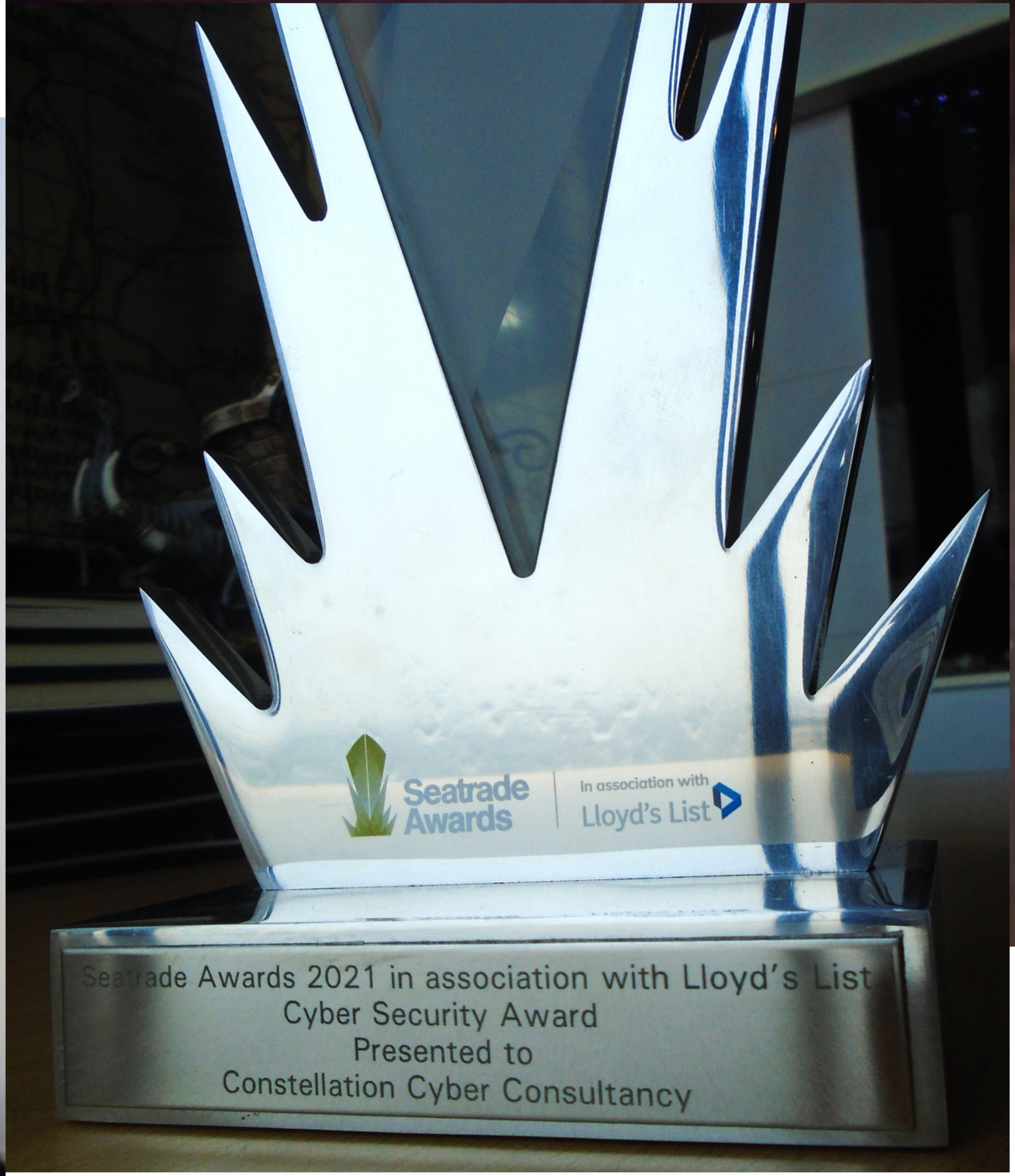
Constellation Cyber Consultancy

in the category

Technology Innovation
Excellence in Cyber Security

Organized by

INNOVATIVE CONCEPTS
WHERE IDEAS STRIKE



Seatrade Awards 2021 in association with Lloyd's List
Cyber Security Award
Presented to
Constellation Cyber Consultancy

SeaTrade Awards 2021 with Lloyd's List

THECYBERCONSULTANCY.COM

CONSTELLATION CYBER CONSULTANCY

Cyber Vulnerability Solutions

Do you have any question?

Find out more about us.

https://thecyberconsultancy.com/

Email us your enquires.

assessment@thecyberconsultancy.com

Hot-Line 24/7

+971 2 671 3320

Download presentation copy

DID YOU KNOW?

"F-35 fighter jets face greater threats from cyber-attacks than from enemy missiles."