VOLUME 4, ISSUE 1

CYBERSECURITY AWARENESS AND EDUCATION

27TH FEBRUARY 2024
The views and opinions expressed in the articles in this Journal are those of the author(s) and do not necessarily reflect the views or opinions of ISO, IEC, JTC 1, SC 27 or the editor of this publication.

ISO, IEC, SC 27, the editor and the authors shall not be liable regarding the use, interpretation or implementation of the material contained in any of the articles contained in this publication.
<table>
<thead>
<tr>
<th>CONTENTS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PROLOGUE</td>
<td>6</td>
</tr>
<tr>
<td>PRESENTATIONS</td>
<td>7</td>
</tr>
</tbody>
</table>
Welcome to Issue 1 (Volume 4) of the ISO/IEC JTC 1/SC 27 Journal. This current issue covers the important topic of cybersecurity awareness and education, the theme of the third International 27001 Day workshop held on the 27th Feb this year. This is a topic that is critical to building a workforce that is aware of the risks related to cybersecurity as well as having a skilled workforce that are skilled in implementing and managing cybersecurity risks. Building an aware and skilled workforce to protect your organization from cyber attacks is primarily a management responsibility, however, every employee of the organization also has an important part to play to implement policies and procedures to protect the organization.

Thanks go to the authors of the workshop presentations and those experts in WG 1 that shared ideas with these authors during the workshop. A special thanks go to our two key-note speakers Natasa Perucica from the World Economic Forum (WEF) and Evangelos Kantas from the European Network Information Security Agency (ENISA) for their time and valuable speeches.

Any questions or feedback relating to the content of this Journal can be directed to editor (sc27.wg1.edwardjh@gmail.com). Also the SC 27 website https://committee.iso.org/home/jtc1sc27/ provides more detailed information on SC 27.

Dr Edward Humphreys
SC 27 Journal Editor, Feb 2024
PRESENTATIONS

- CYBERSECURITY EDUCATION AND AWARENESS IN THE EU - Evangelos Kantas (ENISA)

- THRIVING IN CYBERSECURITY: SUSTAINABLE TALENT PIPELINES - Natasa Perucica (World Economic Forum)

- ISO/IEC 27001, AWARENESS, TRAINING AND EDUCATION – Dr Edward Humphreys

- ISMS AWARENESS AND TRAINING FROM A SWEDISH PERSPECTIVE - Jan Branzell (Veriscan)

- ISMS AWARENESS AND TRAINING FROM A MEXICAN PERSPECTIVE – Pablo Corona-Fraga (NYCE) [this presentation is not yet available - when available it will be included in an updated edition of this Issue]
CYBERSECURITY EDUCATION AND AWARENESS IN THE EU
1. CYBERSECURITY EDUCATION MATURITY ASSESSMENT
OBJECTIVES AND SCOPE

Understand and assess the **maturity level of the MS in cybersecurity education – K12**

**What we focus on:**

- Develop a suitable maturity model for assessing cybersecurity education
- Establish relevant maturity levels for the model and evaluate cybersecurity education in each MS
- Provide recommendations for national initiatives and good practices based on maturity levels and dimensions
METHODOLOGY – DIMENSIONS AND MATURITY LEVELS

Define the elements to be measured, the granularity levels and how they relate to each other, across 3 separate dimensions.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Sub-Dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Governmental</td>
<td>1.1 Regulatory Framework</td>
</tr>
<tr>
<td></td>
<td>1.2 Policies</td>
</tr>
<tr>
<td></td>
<td>1.3 Support</td>
</tr>
<tr>
<td>2. Strategic</td>
<td>2.1 Strategies</td>
</tr>
<tr>
<td></td>
<td>2.2 Action Plan</td>
</tr>
<tr>
<td></td>
<td>2.3 Cooperation</td>
</tr>
<tr>
<td>3. Operational</td>
<td>3.1 Provision of education</td>
</tr>
<tr>
<td></td>
<td>3.2 Uptake of education</td>
</tr>
</tbody>
</table>

5 maturity levels were defined for the model:

<table>
<thead>
<tr>
<th>Maturity level</th>
<th>Score in %</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Non-existent - Low</td>
<td>0-20%</td>
</tr>
<tr>
<td>2. Initial/Ad-hoc</td>
<td>20-40%</td>
</tr>
<tr>
<td>3. Defined</td>
<td>40-60%</td>
</tr>
<tr>
<td>4. Established</td>
<td>60-80%</td>
</tr>
<tr>
<td>5. Optimised/Refined</td>
<td>80-100%</td>
</tr>
</tbody>
</table>
TARGETED CONSULTATIONS

An detailed interview guide was developed, with questions focusing on the governmental, strategic and operational dimensions.

An online survey based on the interview structure was also created to increase participation and facilitate data collection for MS.

Combining the interviews and the online survey, a total of 15 countries were consulted.
**MAJOR OBSERVATIONS**

**Governmental**
- 12 MS have a national policy on cybersecurity education in place or planned
- 5 MS have a regulatory framework implemented
- 6 MS have a national programme in place or planned, while 8 have ad hoc initiatives on cybersecurity education

**Strategic**
- 12 MS consider cybersecurity education as part of their National Cybersecurity Strategy
- Member States have demonstrated a **bottom-up approach to cooperation**, to encourage synergies between the various players, including NGOs, associations and teachers

**Operational**
- **Cybersecurity courses** are delivered to primary and/or secondary school students in all the consulted countries, although only 4 deliver cybersecurity classes as mandatory part of the curricula
- Only 2 MS have implemented monitoring measures, but these are not part of a coordinated monitoring activity defined by an action plan
GOOD PRACTICES FROM MEMBER STATES

Governmental dimension

• Development of a **national policy** or guidelines to guide education stakeholders in their adoption and teaching of cybersecurity topics

• **Definition of a clear governance** and appointment of an entity in charge of supporting teachers

Strategic Dimension

• Enhancement of **national, regional and municipal** cooperation

• Fostering cooperation **between public and private** organisations and across industries

Operational dimension

• Application of **“train the trainer”** approach by training school teachers

• Ensuring **accessibility of cybersecurity courses** by providing different course formats
**RECOMMENDATIONS FOR MEMBER STATES**

<table>
<thead>
<tr>
<th>Governmental dimension</th>
<th>Strategic Dimension</th>
<th>Operational dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Make cybersecurity education binding and a high priority of the government</td>
<td>• Collaborate with universities to offer cybersecurity courses to primary and secondary school students</td>
<td>• Introduce mandatory hours on cybersecurity awareness</td>
</tr>
<tr>
<td>• Have the Ministry of Education help provide access to EU grants and private education initiatives</td>
<td>• Engage teachers in course development and consider the utilisation of a bottom-up and “teach the teacher” approach</td>
<td>• Consider different requirements based on school type, geography and social background of pupils when implementing curricula</td>
</tr>
<tr>
<td>• Implement pilot projects in a reduced number of schools to strengthen cybersecurity in education</td>
<td>• Build a continuous learning path that starts from primary school</td>
<td>• Involve external experts and/or universities in the facilitation of the cybersecurity courses</td>
</tr>
</tbody>
</table>
CENTRAL HUB FOR CYBERSECURITY EDUCATION IN EU

Discover 142 programmes over 26 countries

What do you want to learn?

See all programmes

Computer Science (track in Software Security)

University of Genova
Genova, Italy

Master Degree

English Classroom Charges Apply

Visit Programme’s Website

Share on: Facebook LinkedIn Twitter

• One place to collect information on CS in education
• Central point to exchange good practices
• Sharing of experience
2. AR-IN-A-BOX

TOWARDS AWARENESS CULTURE
“An (internal) marketing strategy designed to raise cyber security awareness.”

✓ Teaches employees how to mitigate the impact of cyber threats.
✓ A plan encompassing multiple awareness-raising activities over a long period of time following the organisation’s strategy for cybersecurity.
✓ It can include one or more internal or external campaigns, focused on a common cybersecurity topic or target group.
WHY HAVE ONE?

➢ New threats are emerging.
➢ Organizations can no longer just rely on their technological defenses to be safe.
➢ Cybercriminals use sophisticated social engineering techniques to by-pass defenses.
➢ All it takes is one employee to click on a malicious link and it’s game over!
➢ Your employees are your first line of defense.

A comprehensive Cyber Security Awareness program is the best way to educate staff and create a security-first culture.
ISO 27001/2 & Information Security Awareness Training

For ISO 27001 compliance, it is essential to comply with clause 7.2.2.

The ISO 27001/2 clause 7.2.2 states:

‘Information security awareness, education and training - All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function’.
NIS DIRECTIVE 2, Article 21: Cybersecurity-Risk management measures

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;
(b) incident handling;
(c) business continuity, such as backup management and disaster recovery, and crisis management;
(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
(f) policies and procedures to assess the effectiveness of cybersecurity risk management measures;
(g) basic cyber hygiene practices and cybersecurity training;
(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
(i) human resources security, access control policies and asset management;
(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.
AR-IN-A-BOX CONTENT

YOUR GUIDE TO DESIGNING A CYBER-AWARENESS PROGRAMME

COMMUNICATION STRATEGIES FOR CYBER AWARENESS

PROMOTION TOOLS AND CHANNELS

CYBER AWARENESS - MEASURING IMPACT

HOW TO RUN THE CYBER-AWARENESS GAME

CYBER CRISIS COMMUNICATION GUIDE

CYBER AWARENESS GAME

EnergyCorp hacked

WHICH TYPE OF CYBER-ATTACK IS COMMONLY PERFORMED THROUGH EMAIL?

A. Phishing
B. Smishing
C. Vishing
D. Ransomware

SCAN ME
DESIGNING A CYBER-AWARENESS PROGRAMME

1. Identify objectives
2. Secure financial resources
3. Ensure human resources
4. Split employees into target groups
5. Choose the right means
6. Create a timeplan
7. Implement program
8. Evaluate the program

AR-IN-A-BOX
YOUR GUIDE TO DESIGNING A CYBER-AWARENESS PROGRAMME
CYBER AWARENESS GAMES

To be added in the EU Academy!
https://academy.europa.eu/
Also available at the ENISA website!
QUIZZES

**Phishing**

CORRECT! The term 'phishing' is used to describe a social engineering based cyber-attack that arrives mainly by email. Though email phishing is the most popular kind of phishing, other variants of this attacks can arrive by SMS (smishing), phone calls (vishing) or ransomware (digital kidnapping).

Other choices: INCORRECT
THANK YOU FOR YOUR ATTENTION

- info@enisa.europa.eu
- www.enisa.europa.eu
Thriving in Cybersecurity: Sustainable Talent Pipelines

World Economic Forum
Centre for Cybersecurity
Contents

01 Why is there a cybersecurity skills gap?

02 How can we bridge the cybersecurity skills gap?

03 What are the focus areas and next steps?
Mind the gap!

At a time when cyber threats are increasing and growing in sophistication, the shortage of cybersecurity professionals leaves organizations vulnerable to disruptions and allows cyberattackers to undermine trust in services that are important for our economies and societies.

There is a global shortage of nearly **4 million** cyber professionals; more than the population of countries such as Uruguay, Armenia, and Mongolia.\(^1\)

**52%** of public organizations state that a lack of resources and skills is their biggest challenge when designing for cyber resilience.\(^2\)

Only **15%** of all organizations are optimistic that cyber skills and education will significantly improve in the next two years.\(^3\)

---

\(^1\)2023 (ISC)² Cybersecurity Workforce Study  
\(^2\)Global Cybersecurity Outlook 2024  
\(^3\)Idem
We launched “Bridging the Cyber Skills Gap” initiative convening 50+ public and private organizations to address the skills and talent gap

Together, we are working to:

**Raise awareness and share knowledge**
Raise awareness and share knowledge amongst C-suite executives and decision-makers about cybersecurity skills deficit and its economic and security implications

**Define strategic approaches on cyber skills**
Define strategic approaches and processes that will help build sustainable cyber talent pipelines within organizations and across sectors

**Showcase success stories and scale opportunities**
Showcases practical examples of successes and best practices from partner organizations in bridging the cybersecurity skills gap and explore opportunities to scale
This initiative is transforming education, skills and learning to prepare 1 billion people for tomorrow's economy and society. Today, 680 million people are on track to receive improved education, skills and economic opportunity by 2030.

“Bridging the Cyber Skills Gap” initiative will build on the Global Skills Taxonomy intended to align around a universal language for skills, and other tools to accelerate how partners identify populations suitable for retraining in cybersecurity.

A common misperception is that all cybersecurity roles and jobs require a computer engineering degree. A skills-first approach has the potential to democratize access to economic opportunities and pathways to good work for many more people than traditional approaches.

“Bridging the Cyber Skills Gap” will build on the Forum's 'Skills-First' work that supports the development of new approaches to talent management. This creates more flexible career paths and widens the talent pool for cybersecurity.
There is a need to develop a strategic **Cybersecurity Talent Framework** featuring actionable approaches to help grow the cybersecurity workforce.
To comprehensively address the different types of shortages and build sustainable cybersecurity talent pipelines, it is imperative to identify and address the underlying reasons that contribute to the broader cybersecurity workforce gap. The "Bridging the Cyber Skills Gap" initiative focuses on:

- Attracting talent into cybersecurity
- Cybersecurity education and training
- Recruitment of cybersecurity professionals
- Retention of the cybersecurity workforce
A lack of understanding for cybersecurity roles and growth opportunities in cybersecurity discourages individuals from pursuing a career in the field.

Moreover, an estimated 78% of organizations report that they do not have the in-house skills to fully achieve their cybersecurity objectives. Talent attraction becomes increasingly competitive with organizations competing for the brightest minds who can drive growth and innovation.

What measures can organizations take to attract talent into cybersecurity?
Irrespective of whether they are intended for K-12 students, university students or professionals, educational programs on cybersecurity face numerous challenges including outdated and misaligned curricula, a shortage of qualified instructors and limited access to mentorship program.

Such setbacks are even further exacerbated by the frequent demand for expensive cybersecurity certifications with varying levels of recognition and relevance.

How can cybersecurity education be improved to reflect cyber reality?
While many cyber skills are transferable, the employers` demand for formal cybersecurity education creates a barrier for entry. In addition, many potential (entry-level) candidates are often discouraged from applying for cybersecurity roles due to extensive requirements listed in job descriptions including certifications and several years of experience.

Data shows that only 25% of cyber leaders feel that their HR teams frequently understand cybersecurity hiring needs to properly pre-screen candidates.

How can organizations rethink recruitment and talent sourcing practices?
Continued stress, fatigue and pressure experienced by cyber professionals results in high attrition, making retention of talent a challenge.

Other factors that lead to resignation in cybersecurity include a lack of appreciation and recognition for cybersecurity staff. The departure of cybersecurity experts not only has financial implications for organizations as they try to replace talent, but it also contributes to loss of invaluable institutional knowledge.

**How can organizations incentivize and retain their talent?**
Thank you

Our dedicated page: https://initiatives.weforum.org/bridging-the-cyber-skills-gap/home
Annex
The Cybersecurity Learning Hub is an initiative designed to tackle the globally cybersecurity skills shortage and democratize access to cybersecurity career paths.

Led by Salesforce with support from Fortinet, the Global Cyber Alliance and the World Economic Forum, the Cybersecurity Learning Hub features training modules on numerous topics such as cyber resilience, artificial intelligence (AI) cybersecurity, and cybersecurity table-top exercises. It also includes a growing library of career-oriented information and expert interviews.

Since its launch in 2019, the Cybersecurity Learning Hub has trained over 1.3 million individuals spread across all continents.
International 27001 Day
Standardization and Awareness
27th February 2024

Dr Edward HUMPHREYS
ISO/IEC JTC 1/SC 27
WG 1 Convenor
ISO/IEC 27001, Awareness, Training and Education

The standard ISO/IEC 27001 (Information security management system – requirements) contains two important areas of requirement:

• Leadership (clause 5) includes resources and support, and responsibilities and authorities for roles relevant to information security;

• Support (clause 7) includes competence and awareness requirements:
  • 7.2 having a competent workforce
  • 7.3 providing workforce awareness
ISO/IEC 27001, Awareness, Training and Education

Standards supporting ISO/IEC 27001 (Information security management system –requirements) relating to awareness and training:

• ISO/IEC 27002 information security controls relating to awareness and training
• ISO/IEC 27003 implementation guidance for ISO/IEC 27001
• ISO/IEC 27005 information security risk management
ISO/IEC Competence Standards

- ISO/IEC 27021 competence requirements for information security management professionals
- ISO/IEC 19896 Competence requirements for information security testers and evaluators
- ISO/IEC TS 23532 Requirements for the competence of IT security testing and evaluation laboratories
ISO/IEC Information Security, Cybersecurity and Privacy Standards

• Complete list of ISO/IEC JTC1/SC 27 standards can be found in SC 27 Committee Document 11
  • https://committee.iso.org/home/jtc1sc27 (Resources)
  • Most of the standards in this document play a part in cyber education, training and awareness
4. Cybersecurity awareness, education and training overview

4.1. Background

As an emerging field, awareness, education and training are the means of acquiring knowledge and skills on a subject. There are several steps in this journey that must be completed by organizations to ensure that their employees are adequately prepared to handle the risks and threats that they may face.

An educational programme should be designed and developed in such a way that it meets the needs of all stakeholders involved. The programme should be designed to meet the needs of the organization, its employees, and other interested parties.

As an organization, its leaders, employees, and stakeholders, it is important to ensure that the program is delivered in a way that is effective and efficient. Training should be tailored to the specific needs of the organization and its employees. It should be designed to meet the needs of the organization, its employees, and other interested parties.

4.2. Awareness

Awareness is a critical component of any cybersecurity program. It is important to ensure that employees are aware of the risks and threats that they may face. Training should be designed to meet the needs of the organization, its employees, and other interested parties.

The stakeholders for the awareness component include a wide range of organizational stakeholders such as management, employees, and customers. Training should be designed to meet the needs of the organization, its employees, and other interested parties.

4.2.1. Education

The main stakeholders for educational programs are universities and other educational institutions, as well as governmental bodies and industry associations. Training should be designed to meet the needs of the organization, its employees, and other interested parties.

4.2.2. Training

Training should be designed to meet the needs of the organization, its employees, and other interested parties. Training should be designed to meet the needs of the organization, its employees, and other interested parties.

5. Cybersecurity skills development

5.1. Competence requirements in the field of cybersecurity knowledge, responsibilities and skills

According to ISO/IEC 27004 competence is defined by knowledge, skills and experience according to the roles and responsibilities a person will have in an organization. ISO/IEC 27004 establishes competence requirements for information security management professionals, and includes related information for developing education and training programmes.

The development of cybersecurity skills is an ongoing process, and it is important to ensure that employees are aware of the risks and threats that they may face. Training should be designed to meet the needs of the organization, its employees, and other interested parties.

5.2. Cybersecurity skills, tools, work roles and responsibilities

This section describes different roles used in organizations regarding cybersecurity activities, these roles are not the same in every organization and should be adapted to the specific context, regional, regulatory and organizational. Annex 1, section 1.2 gives examples of this roles, work roles and responsibilities this section provides an overview of these roles.

5.3. Classroom, laboratory, workplace

There are different techniques and tools used to build and develop a workforce of cybersecurity skills, some of them focused on classic classroom, and other on practice on simulated scenarios or even real situations in the workplace environments.

5.4. Resources and tools

Resources and tools to develop, implement and maintain cybersecurity education and training programs for further development need to be sufficient to develop a range of skills requirements for all levels of specialists and non-specialist topics. This should include having common bodies of knowledge, training scenarios that meet the day to day needs of business and resemble real cybersecurity problems. Tools and corresponding training should enable personnel to familiarize themselves with the use for detection, identification, protection, response and recovery from cybersecurity incidents.

5.5. Annexes

Annex 3 gives examples of tools and other resources available to develop cybersecurity skills.

6. Cybersecurity qualifications

An overview of the different types of cybersecurity qualifications, including academic, professional, and other qualifications can be found in this section.
Thanks for listening

Any questions?

Dr Edward HUMPHREYS  
SC 27/WG 1 Convenor  
Sc27.wg1.edwardjh@gmail.com
Me – Jan Branzell

- Swedish – and live in a city called Karlstad with about 100 000 inhabitants
- Been involved in standardizations since 2000 and within SC 27 since 2003
- Editor for various standards such as ISO/IEC 27003 on guidance of the ISMS requirements, ISO/IEC 27016 on Economics and lately ISO/IEC 27031 on ICT readiness for BCM. Convenor support in JTC 1/WG 13 on Trustworthiness
- Responsible Information and Cyber Security Academy; a program with six 3-day training sessions based on ISO 27000 series by SIS (SE NB)
- Working as a senior consultant with ISMS implementation and enhancements for organization ranging from 10 to over 100 000 employees.

- I have the strong view that standards must be of help to organizations; support their business and not the other way around
Sweden - Basics

- 10,5 M inhabitants
- 447 425,16 km²
- Water 9 %
- (23 inh./km²)

(Source: Wikipedia)
Sweden – Digital maturity – EU data

Global tech things that many of us knows such as "Skype", "Spotify", "Bluetooth"
Big in games: Mojang (Minecraft), Paradox Interactive, EA DICE (Battlefield), Avalanche Studios, King (Candy Crush)
With a rather small society and high technology maturity – you could assume high interest for security awareness....
Swedes and the need of Security – Not that obvious....

History wise a rather closed society – “I know you”

Equality and fairness – “The good state”

Experience of serious conflicts – “Last war in 1814”

Security at the top of the mind?
Awareness in an organization
Start from the top?

Board, Owners, Society etc..

Compliance

Business Requirements

Top Management

Information Security Management (ISM)

Security of Information in Business Processes

Organizational Security
Roles and responsibilities, Rules, Procedures, Dependencies

People Security
Awareness, employment

Physical Security
Facilities, Workplace

ICT Security
Development and Operations Technology

(Source: Veriscan)
Awareness – Age and Technology
A personal reflection based upon my experience...

Assuming Top Management is + 50 y of age
“- Born BC? (Before computer)”

Digital importance on business
Top management awareness

- 1970
- 1980
- 1990
- 2000
- 2010
- 2020
Other factors increases the awareness

- More questions
- Board, Owners, Society etc..
- More requirements
- More regulations
- Compliance
- Business Requirements
- More questions from the personnel

More awareness of ISO/IEC27001 “ISMS” as a solution by Top Management
The situation has changed and is changing fast. Security awareness is now a concern for many Swedes...
## Awareness initiatives

<table>
<thead>
<tr>
<th>Level</th>
<th>Actors</th>
<th>Target audience</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>National</td>
<td>Swedish Civil Contingencies Agency</td>
<td>The society in general</td>
<td>(There are also other governmental agencies that is more related to defence)</td>
</tr>
<tr>
<td>National</td>
<td>SIS (SE NB)</td>
<td>Professionals within security</td>
<td>Information and Cyber Security Academy</td>
</tr>
<tr>
<td>Regional</td>
<td>21 County Administrative Boards</td>
<td>Local infrastructure</td>
<td>Coordination of organizations and training – Mostly defence</td>
</tr>
<tr>
<td>Educational</td>
<td>Universities</td>
<td>Students and in some cases organizations</td>
<td>Cooperates sometimes with Regional actors</td>
</tr>
<tr>
<td>Organization</td>
<td>Public/ Private sectors</td>
<td>People within the organization</td>
<td>Every organization is unique</td>
</tr>
</tbody>
</table>
What can private individuals do?

Everyone living in Sweden can contribute to our general preparedness and security. You can avoid spreading false rumours, stay prepared at home or get involved in other ways.

Keep a cool head, don’t spread rumours

Sweden may experience an increased risk of cyber-attacks and attempts to disinform and spread rumours. You can help to counter these measures by:

- Remaining alert for misinformation and not spreading it further.
- Seeking information from credible sources. The website krisinformation.se provides updated and accurate information from public authorities and organisations.

Protect your data from cyber attacks

If an IT attack occurs, an attacker must have found a security hole. But you can protect your data and contribute to society’s cyber defence with a few simple steps:

- Install security updates on your phone, computer and other devices as soon as possible.
- Use services with reliable encryption for calls and messages, there are several of them including “Signal” and “Cryptify”. Please consult the Swedish Post and Telecom Authority (PTS) for further guidance.
- Be wary of phishing attempts and attempts to plant malware, for example via web pages or links in emails or text messages.
- Protect your eID.

Get involved
Example: National

Makes a lot of publications

Youtube films
Example: National SIS Information and Cyber Security Academy

**Basic level**
ISO/IEC 27000, 27001, 27002, 27003

**Basic 1**
3 days

**Basic 2**
3 days

**Extended level – Free choice**
ISO/IEC 27000, 27001, 27002

**PLUS ++++**

**ISMS Implementation**
“27003”, “27016”, “27005”
3 days

**ISMS Enhancement**
“27003”, “27016”
3 days

**Audit**
(ISO 19011. ISO/IEC 27006/07/08)
3 days

**Risk, BCM, Incident**
ISO 31000, 22301
ISO/IEC 27005, 27035, 27031
3 days

Started in 2009 and have had over 2000 attending
Example education:
University of Skovde/School of Informatics

Basic education programmes:
- Network and system administrator (NSA)
  - Risk assessments based on ISO/IEC 27005
- Cybersecurity and Network Administration (CNA)
- Introduction to information security (ISO 27000 standards)

Advanced programmes:
- Privacy, Information security and CyberSecurity (PICS)
  - Includes ISMS with 27001, 27002 and 27003
- Assignment programmes
  - (Based upon input from regional initiatives)
    - 1 year programme for employees at different organizations such as CISOs
    - Based upon 27001, 27002 and 27003

The long-term view is to integrate information security in all different fields
Organizations “What”:

**What kind of awareness?**
- ”Do not click”
- This is why security is important for us! (Policy)
- This is what you should do (”our rules”)
- ”Create” a security culture

To prevent a certain threat
To create understanding
To know the rules
To “act” together

Security culture – you always have one. But is it right?
Organizations “How”:

To prevent a certain threat

- Smaller organizations – Information by CISO
- Larger organizations – “tests”

To create understanding

- Smaller organizations – Information by CISO and CEO
- Larger organizations – Awareness programmes – Films, Intranet

To know the rules

- Smaller organizations – Information by CISO and CEO
- Larger organizations – Awareness programmes – E-learning + tests

To “act” together

- Smaller organizations – Working with ISO/IEC 27001 standard “Proud”
- Larger organizations – All above combined + “ISMS” systematic approach
Awareness starts at the top – Involvement for time and money!
THANK YOU!

Veriscan Security Sweden AB
www.veriscan.se

Feb 27th 2024