# Review of Cyber Hygiene practices

DECEMBER 2016

www.enisa.europa.eu

European Union Agency For Network and Information Security

# About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

## Contact

For media enquires about this paper, please use press@enisa.europa.eu.

### Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

### Copyright Notice

ISBN 978-92-9204-219-6, DOI 10.2824/352617

# Table of Contents

# Executive Summary

Cyber hygiene plays a critical role across the EU in protecting businesses, but it also provides the foundations for protecting the infrastructure and customer data which businesses rely on. This importance is recognised within the European Union to the extent that almost all the Member States have developed a national cyber security strategy[1] which aims to improve, and enhance, the way organisations protect themselves from cyber threats.

Unfortunately, despite the national strategies, this has rarely translated into direct cyber hygiene programs targeted at businesses in a manner which provides guidance around what constitutes good practice and why only three such hygiene programs were found in the EU.

The general trend from respondents in this survey was that cyber hygiene may be a good idea, but it is generally quite low priority for most businesses unless there is a pressing, external, need to comply. The most common forms of this are business to business contract terms and governmental regulations. Without this form of pressure, it is unlikely that there will be significant take-up of any cyber hygiene scheme.

Businesses, especially small to medium enterprises, perceive they get the most benefit from cyber hygiene programs which allow them to achieve a demonstrable certification and request a demonstrable certification from their supply chain. This generates a measurable return on investment, justifying any resource cost required by the increased security.

One key part of security missing from all three European guides, but captured in the USA program, is the use of a risk-based approach. In the European programs there is little if any guidance for business owners with regards to assessing their individual risks, identifying high-risk assets and scaling their security to implement a “crown jewels[2]” type approach. While this may be challenging for small businesses, excluding it entirely forces organisations into a one-size fits all approach. In turn, this may lead to excessive implementation or operational costs for the cyber security program.

The key recommendation from this report is that there needs to be a standard approach to cyber hygiene across all the European Union. The European Commission should set the standard of minimum baseline requirements for cyber security. Additionally, this approach should be flexible enough that Member States can enhance areas which are important to them but should still support cross-border and cross-industry recognition.

To be effective this approach needs to be attainable, accreditable and affordable. The affordability is likely to be the most important aspect for any business but all three will work in conjunction to drive engagement.

[1] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

[2] For more on this see https://www.securityforum.org/tool/protecting-the-crown-jewels/

# 1. Introduction

Cyber attacks are growing in both frequency and impact[3]. The repercussions of security mistakes often end up being headline news and can cause significant harm to the victim organisation. However, there is a perception that only big, global, corporations are at risk and, as a result, thousands of attacks against the Small – Medium business sector go largely unreported.

Most successful attacks leverage well known security problems. Reporting from the UK Government's CESG (the part of GCHQ tasked with protecting the nation) indicates that around 80% of cyber attacks[4] are the result of poor cyber habits within the victim organisations.

To address this, a cyber hygiene strategy should be implemented which emphasises the importance of carrying out regular, low impact security measures. This will minimise the risks of becoming a victim of a cyber attack or spreading the impact of a cyber attack to other organisations.

In this context, cyber hygiene should be viewed in the same manner as personal hygiene and, once properly integrated into an organisation will be simple daily routines, good behaviours and occasional check ups to make sure the organisations online health is in optimum condition.

As businesses across Europe become more connected, with multi-level supply chains for even the smallest organisation, this last point becomes quite significant. The attack on the US Target corporation in 2013, for example, was the result of a compromised vendor within their supply chain[5]. While this has highlighted the need to secure the supply chain, most SMEs struggle to have the resources, access or knowledge to do this properly. In turn, this places a greater emphasis on cyber hygiene to help businesses protect the entire community as well as themselves.

This report looks at the leading cyber hygiene programs across the European Union and drills down into a selection of Small – Medium Enterprises to establish their understanding and engagement with the national strategies. Based on the information provided by the organisations, this report also looks to draw conclusions leading to recommendations on how cyber hygiene can be improved across Europe.

[3] https://www.enisa.europa.eu/publications/etl2015

[4] https://www.gov.uk/government/news/cyber-security-boost-for-uk-firms

[5] https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

# 2. Overview of Leading European Cyber Hygiene Programs

Currently there is no single standard or commonly agreed approach to cyber hygiene across Europe with each of the Member States having their own programs and guidance. Predominately, these programs are aligned to, or driven by, the National Cyber Security Strategies published by each Member State[6] and are at varying levels of maturity.

Within the publicly available documents, three programs can be identified as developed enough to give specific advice to businesses. These are the programs from Belgium, France and the United Kingdom.

In addition to this, the United States National Institute of Science & Technology (NIST) produces a guide for small business security and this is reviewed at a high level below.

## 2.1 Belgium

### 2.1.1 *Belgian Cyber Security Guide*[7], produced by a public-private sector partnership[8].

This is a high level, informational guide designed to provide advice on good practices around cyber security controls. The guide is designed to be industry and technology agnostic. The publicly available version of this document does not carry any indication of when it was last published or when a change is due.

The guide is split into two main parts. The first part identifies 10 Key Security Principles which should be adopted by every business (See Annexe A). This is followed by 10 “must do” security actions which look to turn the principles into more accessible guidance. Following this, there is a self-assessment (SA) questionnaire which aims to allow users to drill into each principle/action area to get a better view of what they need to consider for their organisation. There are 16 high level question areas with 5 questions in each, and users can provide 3 answers broadly equating to “*we do this properly, we could improve, and we are bad at this*.”

To further facilitate ease of use, each SA question is clearly linked to the relevant principles and must-do actions.

Although there is no formal, externally verified, certification scheme linked to this Guide, it is possible that the SA questions could be used as an attestation document during a security assessment exercise.

## 2.2 France

### 2.2.1 *40 Essential Measures for a Healthy Network*[9], produced by ANSSI[10].

This is a foundational guide covering 13 control areas and seeking to drive a defence in depth approach. Each of the essential measures are effectively rules building what ANSSI believes is the minimum baseline for security. There is some latitude available to end users as the guide does not mandate

[6] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map
[7] Available from https://www.b-ccentre.be/wp-content/uploads/2014/04/B-CCENTRE-BCSG-EN.pdf
[8] The guide has been produced by ICC Belgium, FEB, EY, Microsoft, L-SEC, B-CCENTRE and ISACA Belgium
[9] Available from https://www.ssi.gouv.fr/uploads/IMG/pdf/guide_hygiene_v1-2-1_en.pdf
[10] Agence nationale de la sécurité des systèmes d'information

specific implementations or technology choices. Initially produced in 2013, the 40 measures are due for their next update in 2017.

The control areas chosen by ANSSI (see Annexe B) are geared around standard office systems (separate guidance is available for SCADA / ICS systems) and are driven by ANSSI research which indicates that following these rules would have prevented a significant number of attacks they have dealt with.

ANSSI currently have no mechanism by which organisations can verify compliance with the 40 essential measures or use these rules to demonstrate good cyber hygiene practices to other businesses.

### 2.2.2 *Guide Des Bonnes Pratiques De L'informatique*[11], produced by CGPME / ANSSI.

Because of the size and perceived complexity of the 40 rules, a cut down version of 12 rules has been produced to assist small to medium size enterprises in France. Unlike the 40 Essential Measures document, this is only publicly available in French which limits is applicability across Europe.

The good practice guide is accessible to both IT professionals and non-experts alike. This is a good reflection of the variety among the small to medium enterprise sector and each section (rule) starts with a scenario designed to be immediately relatable for the small business owner.

In the same manner as the 40 essential measures, there is no accreditation, verification or compliance assessment scheme for the 12 rules within the good practice guide.

## 2.3 United Kingdom

### 2.3.1 *Cyber Essentials*[12], produced by the UK Government.

The UK Government, supported by the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF), developed the Cyber Essentials guidance to identify the basic technical controls required to defeat the vast majority (estimated to be around 80%) of cyber attacks detected by the national security agencies.

Highlighting the "essentials" element of the scheme, there are only 5 control areas (see Annexe C) and the emphasis is very much on physical infrastructure controls – cloud services and application layer security controls are largely excluded from the scheme.

Cyber Essentials has been designed to provide a "certification" scheme by which companies adhering to the guidance can be verified and demonstrate compliance to customers and business partners. There are currently two levels of certification – a self-attestation version, similar to the Payment Card Industry SAQ, and an independently technically verified version (called Cyber Essentials Plus). Successful certification allows businesses to put the Cyber Essentials logos on their business documents & websites.

Certification is handled by the private sector. Currently four accreditation bodies are appointed by the Government to manage the activity of certification bodies, who in turn are responsible for delivery of certification services to the end customer.

[11] Available from https://www.ssi.gouv.fr/uploads/2015/03/guide_cgpme_bonnes_pratiques.pdf

[12] Available from https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

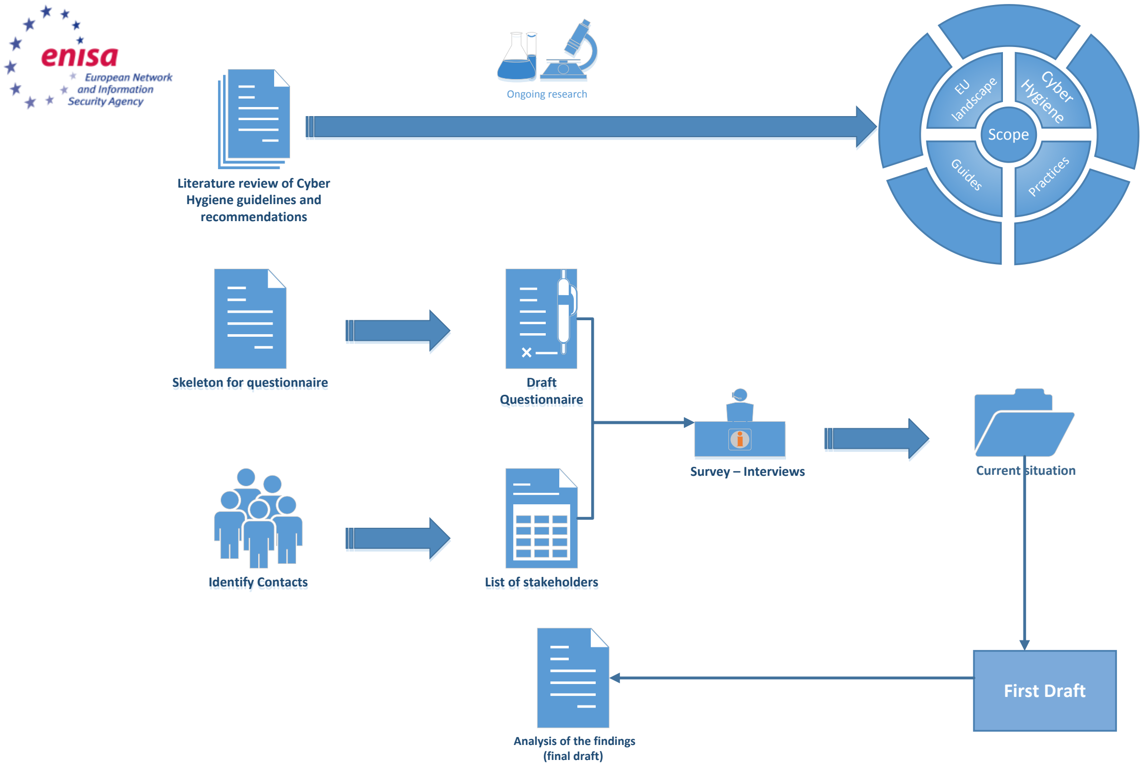
Launched in June 2014, certification against the Cyber Essentials scheme became a mandatory requirement for Government contracts handling sensitive information in October 2014. Partly as a result of this, as of October 2016 there are approximately 4000 certified companies.

# 3. Methodology

This report uses a two-stage research approach. In the first part, a desktop search was conducted to establish what information was publicly available regarding cyber hygiene programs. This was followed up by engagement with representatives from ANSSI and the UK government to get specific details on the national schemes.

The second stage was a series of interviews with small-medium businesses in the UK to establish the level of engagement with the national cyber hygiene program and the level of understanding within the business around general cyber security issues. These interviews used a pre-determined questionnaire to standardise responses. To maximise the value from the second stage, businesses were selected from a range of industries and geographical regions within the UK. To encourage open and honest responses, it was agreed with the interviewees that their names, and their business identities, would be withheld from the final report.

On completion of the interviews a qualitative assessment was carried out to establish patterns within the responses and determine overlaps between industry sectors and organisational size.



# 4. United States National Institute of Science and Technology

In November 2016, the US National Institute of Science and Technology (NIST) published NISTIR 7621 Revision 1 “Small Business Information Security: the fundamentals[13].”

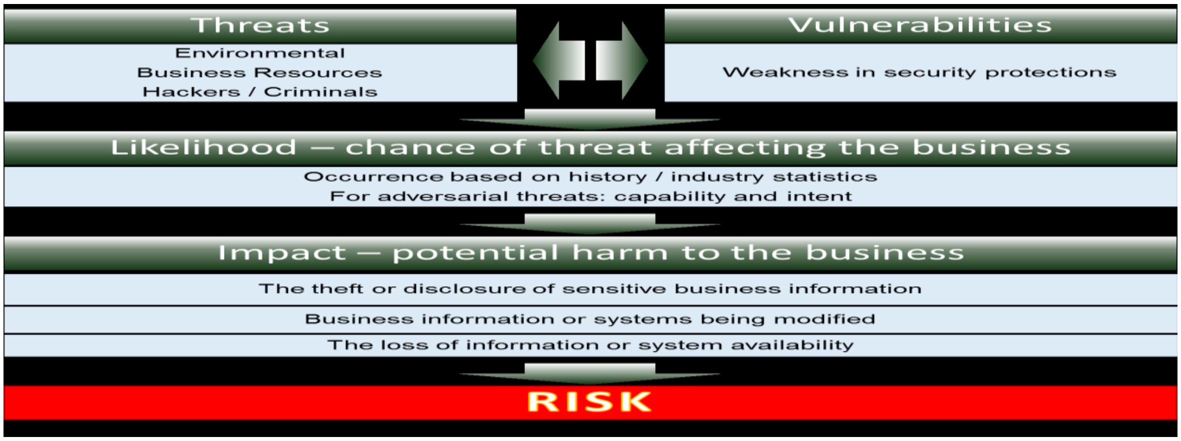
This publication is a guide to help small businesses apply basic security controls to their information, systems and networks. The guide itself is organised into sections which assist the user on a logical flow through a risk managed approach to cyber security.

In general, this program contains enough advice for reasonably skilled IT workers in a small business to apply some good practice controls (e.g. passwords should be set to at least 12 characters) without forcing the business to implement a specific technology.

Unusually for a small business cyber security program, this guidance also includes advice on risk management and worksheets. These assist the business in determining the value of their information assets and prioritising security controls in a reasonably straight forward manner.

Like the Belgian and French guides, the NIST document is an advisory publication. There is no associated scheme which allows businesses to certify their compliance or use certifications to reduce the supplier security assessment burden.

In October 2016 legislation was introduced to combat cyber attacks against U.S. computer networks. The Promoting Good Cyber Hygiene Act[14] builds on President Obama’s 2013 Executive Order[15] by instructing the National Institute of Standards and Technology, in consultation with the Federal Trade Commission and the Department of Homeland Security, to establish voluntary best practices for network security, such as not using a default password and regularly applying software updates. Figure 1: How risk is determined for businesses


Threats
Environmental
Business Resources
Hackers / Criminals
Vulnerabilities
Weakness in security protections
Likelihood — chance of threat affecting the business
Occurrence based on history / industry statistics
For adversarial threats: capability and intent
Impact — potential harm to the business
The theft or disclosure of sensitive business information
Business information or systems being modified
The loss of information or system availability
RISK

[13] Available from http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
[14] https://www.congress.gov/bill/114th-congress/house-bill/3664
[15] http://eshoo.house.gov/issues/economy/eshoo-bill-vaccinates-against-majority-of-hacks-with-cyber-hygiene-network-security-management/

# 5. Research Findings

Analysis of the questionnaires has led to the following key findings:

- There is no unified, pan European approach to cyber hygiene programs.
- While there isn't a consistent set of requirements for a cyber hygiene program, there are sufficient overlaps to identify some key control areas which should be included in any program.
- None of the UK SME's interviewed initially recognised the term *cyber hygiene* and this had to be explained to put the questionnaire in context.
- Each nation within Europe has its own Cyber Security strategy which drives the direction of cyber hygiene and as would be expected from the topic, there are overlaps in the choice of controls. However the approval of the NIS Directive will pave the way towards homogeneous cyber security strategy's across the European Union.
- There is no simple mechanism by which a business in one Member State can demonstrate cyber hygiene compliance to a business/customer in a different Member State without adhering to multiple programs simultaneously.
- The Member State guidance around cyber hygiene is almost entirely advisory with no obligations to implement the controls or sanctions for any security failures – with the exception of failures leading to personal data breaches.
- The UK Government has implemented a policy of requiring compliance with its cyber hygiene program (cyber essentials) for businesses delivering services which has driven adoption of the program.
- Every organisation questioned identified the need to factor in the cost of a cyber hygiene program against the perceived benefits. In some instances, this led to decisions against adopting a security program.
- Every SME interviewed who has implemented a cyber hygiene program, has done so because of a legal or contractual requirement to do so. None of the organisations interviewed have implemented good security practices to simply protect themselves properly.
- There is a direct correlation between the size of the organisation and the awareness of IT Security risks. Once an organisation becomes large enough to dedicate someone to manage IT, there appears to be at least a baseline awareness of good security practices.
- Small businesses are unwittingly carrying a significant risk regarding their cyber hygiene practices and appear to think it doesn't affect them because they are so small.
- SMEs who operate outside traditional IT-based industries have very limited awareness of the importance of IT to their business, this is especially acute when considering the impact of a security incident.

- The UK has a government backed cyber hygiene program, which is mandatory for most public-sector contracts and which shows strong public sector support. Unfortunately however there is still very limited awareness of the scheme at the time of writing.
- The UK Cyber Security Forum[16] scheme is a promising development and should increase cyber hygiene awareness within the SME sector, but this still has limited penetration.
- The main pain point for all businesses is finding a simple, cost effective way to improve their security which can be understood by non-technical people.
- The main additional pain point for businesses as they grow in both size and structure, is securing the supply chain.

[16] http://www.ukcybersecurityforum.com/index.php/cyber-security-clusters

# 6. Conclusions

## 6.1 Cyber hygiene

Cyber hygiene is a fundamental principle relating to information security and, as the analogy with personal hygiene shows, is the equivalent of establishing simple routine measures to minimise the risks from cyber threats. The underlying assumption is that good cyber hygiene practices can drive increased immunity across businesses reducing the risk that one vulnerable organisation will be used to either mount attacks or compromise a supply chain.

While this appears well understood at the national level, and almost all European Union Member States have now developed a National Cyber Security Strategy, this does not translate well to the small – medium enterprise sector.

The variation between national standards leads to uncertainty and, given the overlap between both Member State programs and global security standards, confusion over what needs to be implemented.

This is a critical issue as a uniform approach to cyber hygiene which allowed businesses to establish security trust across national borders would drive improvements across the board and effectively develop a cyber version of increased immunity to common attacks.

### 6.1.1 Recommendations

The European Commission should promote cyber hygiene schemes, particularly those targeting Small and Medium sized Enterprises, throughout the EU. In addition, the Commission should foster a common approach to the core messages across all member States.

ENISA should consider establishing a pan-European set of guidelines to act as the minimum baseline requirements for cyber hygiene and would allow Member States to build their own programs on top of this.

To provide value, these guidelines must enable companies (or government bodies) in one Member State to trust the implementation of the controls by a company (or government) in another.

## 6.2 Good cyber hygiene practices – a standard approach

Overall, the existing schemes present three different views of cyber hygiene with enough areas of overlap to indicate what should be considered general good practice.

Unfortunately, these good practices are rarely fully implemented across business sectors and this creates a gulf between the “theoretical” guidance from the standards and the “practical” experience of small-medium business owners and managers.

This has led to some confusion between standards. In the UK this is most noticeable when respondents compare Cyber Essentials, which is essentially a good practice guide, with ISO 27001 which is a way of assessing an Information Security Management System. Although some appear to think there is a decision to be made between these standards, the reality is compliance with one, assists compliance with the other.

### 6.2.1 Recommendation

If implemented, the standard approach to cyber hygiene should cover the following main topic areas, which would also give scope for individualisation by Member States or industry sectors, while retaining the ability to establish compliance regimes:

1. Protect the perimeter
2. Protect the network
3. Protect individual devices
4. Use the cloud in a secure manner
5. Protect the supply chain

Based on these five areas, one approach, similar to the existing regimes, would be to break down into 10 action points:

1. Have a record of all hardware so you know what your estate looks like
2. Have a record of all software to ensure it is properly patched
3. Utilise secure configuration / hardening guides for all devices
4. Manage data in and out of your network
5. Scan all incoming emails
6. Minimise administrative accounts
7. Regularly back up data and test it can be restored
8. Establish an incident response plan
9. Enforce similar levels of security across the supply chain
10. Ensure suitable security controls in any service agreements (including cloud services)

In order that small businesses would consider adopting this standard, there are three key aspects which must be considered during the creation of the controls:

#### 6.2.1.1 Attainable

The good practice requirements should be measures which can be implemented by businesses with limited, or no, dedicated IT Security personnel. It is not realistic to expect a small business to be able to hire a coding expert to deploy bespoke monitoring and alerting scripts, and this level of detail is excessive for a foundational standard.

Good practice controls should be aimed at measures which can be achieved by standard operating systems or applications, or through minimal business processes. This can be enhanced with technology for organisations facing a more powerful threat, but the enhancements should be optional to the standard.

#### 6.2.1.2 Accreditable

The real value for most businesses from a cyber hygiene program is the benefits it can bring. This can be as simple as a way of advertising to customers and clients that they take security seriously, therefore acting as a market differentiator, or as complicated as allowing them to streamline the security aspects of due diligence checks.

In the UK, the primary driver of Cyber Essentials is its role in allowing businesses to retain and deliver contracts with various government agencies. This drives two benefits: the cost of certification is offset by the value of the contract; and the government agency can reduce the resource burden of accreditation.

By being accreditable, a cyber hygiene program provides immediate benefits and encourages businesses to pass on the improved security in their own contracts. In the European Union context, this would require the accreditation system to allow cross border checks to ensure equivalence independent of Member State requirements.

#### 6.2.1.3 Affordable

Cost is likely to be the ultimate deciding factor for any organisation considering adopting a cyber hygiene program. While the lifetime cost of any program might be significantly less than the cost of a breach, this is unlikely to sway small businesses concerned about immediate cashflow.

Engagement from the smaller businesses will need more than guidance about return on investment, it will need the costs of compliance to be low enough that any impact is negligible.

In practical terms, there are three aspects to the cost of a scheme:

**Cost of Implementation** – this cost impacts any organisation looking to adhere to the requirements and is manifest in any new technology, service agreements or support contracts required. It is difficult to anticipate what this will be, but by reducing the need for specific applications or tools, this can be minimised. A standard which makes extensive use of built in controls and permits free choice in any new tooling, will also minimise the implementation costs.

**Cost of Accreditation** – this is a cost which is only carried by organisations who need to achieve certification for a business purpose. Thus, the cost is likely to be compared against the possible benefits the certification brings. In the UK, accreditation to the Cyber Essentials scheme costs £300 (approximately €350) per year which may seem trivial to a company bidding on a five-figure government contract. Ultimately in a publicly managed scheme the cost of accreditation will be dictated by the value the certification offers and the cost of administering a system.

**Cost of ongoing maintenance** – this is the cost necessary to maintain the scheme and to ensure that it is kept up to date and reflects changes in the threat environment. This is a long-term commitment that needs to be factored into the business plans.

## 6.3 Cyber Security Awareness

Organisations without a dedicated, and separate, IT function demonstrated very limited understanding around cyber security in general. Where organisations operate on a business to business line, there is a tendency to implement controls as required by contracts and for business to customer organisations, there doesn't appear to be a clear driver around why security adds value.

Even though the UK Government is trying to drive Cyber Essentials, there is almost no awareness of the program within small businesses unless they have already attempted to gain government contracts. This indicates that while the scheme may be effective, it isn't driving good practice across all industries.

The current trend within the national awareness programs is to have the information available on request and it was apparent from the small businesses that most do not have the awareness to seek out advice, even if they had the technical knowledge to consume it.

This issue is highlighted by a small retail respondent who thought cyber security didn't matter because they didn't sell goods online. They were not aware of the risks from an attacker using their administrative computers to steal funds, change orders or attack other businesses.

### 6.3.1 Recommendations

Member States should be encouraged to have a stated policy of driving awareness to the small-medium business sector rather than rely on providing information for those who search for it. If given more support, a model like the UK Cyber Security Forum / Cyber Security Clusters may achieve this at a *grassroots* level.

This should include educating the SME sector to understand how important all technology assets are to a modern business and on the importance of good practices on all IT assets.

## 6.4 Conflicting Requirements

Although there is foundational overlap between the various national standards, there are sufficient differences that some organisations, especially those without dedicated IT resources, find it challenging to map between standards. This creates challenges for organisations seeking to deliver goods or services across geographical borders as there is a perception that compliance in one country isn't the same as compliance in another.

This leads to an additional difficulty faced by companies with cross border supply chains. Supplier security assessments become resource intensive, time consuming and costly with limited confidence as to the level of risk management they provide.

For a small business, the difficulty in properly verifying supplier security frequently leads to this being neglected without a real understanding of the associated risks.

One positive point raised about the UK Cyber Essentials scheme is that the process makes it easier for businesses to rely on the certification body to carry out the checks. This appears to have been the main driver for the UK government mandating certification for companies winning defence contracts.

### 6.4.1 Recommendation

Any EU wide cyber hygiene scheme should have a mechanism for companies to certify their compliance with the scheme in a manner which is trusted by other companies and government bodies. This immediately generates value for both the company getting certification and the company requiring it across the supply chain.

## 6.5 Combined Public and Private Sector Engagement

Most organisations interviewed were unaware of the Government established cyber hygiene schemes and the existence of Cyber Essentials was not enough for them to become interested. Additionally, there appears to be little appetite to enhance security for the sole purpose of protecting the organisation.

The primary drivers for businesses to adopt good cyber hygiene practices were almost entirely in direct response to a set of contractual requirements. Given the lack of interest in self-protection, it is therefore concluded that the most effective way to encourage good cyber hygiene is to ensure it is enshrined in unavoidable obligations.

It was also noted that the more mature an organisation appeared to be with regards to cyber security, the more likely they would force security controls across their supply chain through the use of enforceable contractual clauses.

### 6.5.1 Recommendation

A two pronged approach should be used to maximise engagement and minimise perception that this is government overreach.

Member State governments should be encouraged to establish requirements around the minimum viable security an organisation should take, aligned to the cyber hygiene standards recommended above.

However, private sector organisations should also be engaged to embed good cyber hygiene into standard contract terms. Ideally this would be through engagement with business groups, chambers of commerce and similar structures. This may be assisted if the accreditation of the standard is managed by a private sector body with Member State government's approval.

## 6.6 Cyber security is perceived to be expensive

Profitability and profit margins are an overwhelming concern for every business interviewed. Most noticeable within the small business sector is the perception that following any sort of good security practices will erode profits.

This is possibly driven by the effort organisations have to absorb to achieve ISO9001 certification and the headline costs of ISO27001 certification which can be unacceptable to a business operating on small margins.

Based on the technological awareness of the organisations surveyed, it is also concluded that this perception of cost is driven by the belief that good security practices need expensive tools or skilled professionals on the payroll.

### 6.6.1 Recommendations

Any Member State or pan-European cyber hygiene standard should strive to minimise the requirement for expensive security controls.

Effort should be made to avoid specifying a particular technology, and controls should be achievable using built in Operating System tools wherever possible.

## 6.7 Lack of cloud security controls

All the existing national cyber hygiene programs focus very heavily on managing and protecting physical infrastructure. This is most apparent in the French and UK programs where most controls assume the business is directly managing the assets.

This creates a problem for organisations who want to adhere to the guidance but have adopted a cloud-based service model where they aren't directly able to carry out administrative tasks such as ensuring patches are applied.

While security professionals may quickly realise how to adapt the programs to service environments, this is less likely for small businesses without specialised resources.

### 6.7.1 Recommendation

ENISA should advise Member States to adopt the Cloud Security Guide for SME[17]s as part of their national cyber hygiene programs. This can enable businesses looking to migrate into cloud services to ensure good practices are verified in advance and confirmed by contractual commitments.

## 6.8 Risk management

The three European programs provide a generic set of controls with, in the case of the Belgian & UK, a set of requirements to meet each control. While this can be effective it does set an arbitrary baseline and a business owner may not feel they have latitude when it comes to implementing a security control.

This effectively eliminates the function of risk management within the cyber hygiene programs and may lead to organisations taking an all-or-nothing approach.

While this may only be applicable to a limited number of SMEs, it has the potential to undermine adoption and lead to users believing the program is more a compliance exercise then adding genuine security value.

### 6.8.1 Recommendation

Any standard approach to cyber hygiene needs to advise users on risk management and allow a scaled response to security threats. Ideally this would be based on the US NIST model of advising the users on how to grade their assets then giving them latitude to create defence in depth with their security controls.

## 6.9 Limited research cover

The current state with fragmented cyber hygiene programs made it challenging for this research to cover more than a small sample of Member States.

### 6.9.1 Recommendation

Further research to identify the understanding of cyber hygiene and resulting approach to security should be conducted to specifically target businesses in Member States without a documented cyber hygiene program.

[17] https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

# Annex A: Cyber hygiene Practices Across Europe

## A.1 Belgian Cyber Security Guide – 10 Key Security Principles

Principle 1: Look beyond the technology

Principle 2: Compliance is not enough

Principle 3: Translate your security ambition into an information security policy

Principle 4: Ensure top management commitment

Principle 5: Create a visible security role in your company and embed personal responsibility

Principle 6: Remain secure when you outsource

Principle 7: Ensure security is an enabler for innovation

Principle 8: Keep challenging yourself

Principle 9: Maintain focus

Principle 10: Be prepared to handle security incidents

## A.2 Belgian Cyber Security Guide – 10 “Must-Do” Security Actions

Action 1: Implement user education & awareness

Action 2: Keep systems up to date

Action 3: Protect information

Action 4: Apply mobile device security

Action 5: Only give access to information on a “need to know” basis

Action 6: Enforce safe surfing rules

Action 7: Use strong passwords and keep them safe

Action 8: Make and check backup copies of business data and information

Action 9: Apply a layered approach against viruses and other malware

Action 10: Prevent, detect and act

# Annex B: Cyber hygiene Practices Across Europe

## B.1 ANSSI 40 Essential Measures for a Healthy Network – Control Areas

The ANSSI 40 measures are broken down into 13 control areas as follows:

1. Know the System and its Users
2. Control the Network
3. Upgrade Software
4. Authenticate the User
5. Secure Computer Terminals
6. Secure the Inside of the Network
7. Protect the Internal Network from the Internet
8. Monitor Systems
9. Secure Network Administration
10. Control Access to the Premises and Physical Security
11. Organise Response in the Event of an Incident
12. Raise Awareness
13. Carry Out a Security Audit

## B.2 CGPME Guide des Bonnes Pratiques De L'informatique (Good Practice Guide)

The 12 essential rules are in the following areas (with approximate translations from French)

| | | |
|---|---|---|
| 1. | Choisir avec soin ses mots de passe | Choose your passwords carefully |
| 2. | Mettre à jour régulièrement vos logiciels | Regularly updates your software |
| 3. | Bien connaître ses utilisateurs et ses prestataires | Know your users and providers |
| 4. | Effectuer des sauvegardes régulières | Make regular backups |
| 5. | Sécuriser l'accès Wi-Fi de votre entreprise | Secure your company's Wi-Fi access |
| 6. | Être aussi prudent avec son ordiphone (smartphone) ou sa tablette qu'avec son ordinateur | Secure your mobile devices (Smartphones / Tablets) |
| 7. | Protéger ses données lors de ses déplacements | Protect your data while on the move |
| 8. | Être prudent lors de l'utilisation de sa messagerie | Be careful when using your mail |

| | | |
|---|---|---|
| 9. | Télécharger ses programmes sur les sites officiels des éditeurs | Download software from official sites |
| 10. | Être vigilant lors d'un paiement sur Internet | Be vigilant when paying over the Internet |
| 11. | Séparer les usages personnels des usages professionnels | Separate personal and business use |
| 12. | Prendre soin de ses informations personnelles, professionnelles et de son identité numérique | Take care of personal, professional information and digital identities. |

# Annex C: Cyber hygiene Practices Across Europe

## C.1 UK Cyber Essentials Scheme – Control Areas

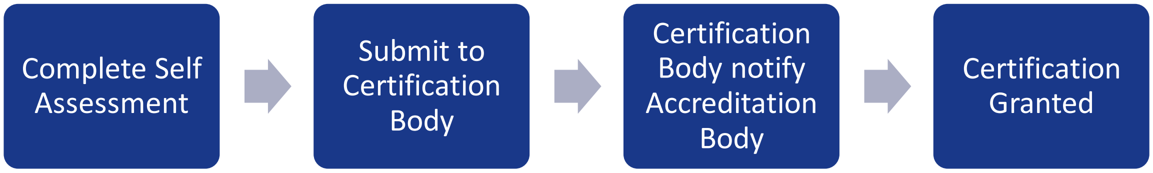
1. Boundary Firewalls and Internet Gateways
2. Secure Configuration
3. User Access Control
4. Malware Protection
5. Patch Management

## C.2 Certification Levels

Cyber Essentials – Self Assessment Form submitted with evidence to Certification Body

Cyber Essentials Plus – As above plus independent technical verification

## C.3 Certification Process Overview


Complete Self Assessment
Submit to Certification Body
Certification Body notify Accreditation Body
Certification Granted

# Annex D: Cyber hygiene Practices Across Europe

## D.1 High Level Recommendations for a Standard Approach to Cyber Hygiene

### D.1.1 Five Key Control Objectives

1. Protect the perimeter
2. Protect the network
3. Protect individual devices
4. Use the cloud in a secure manner
5. Protect the supply chain

### D.1.2 10 Foundational Cyber Hygiene Tasks

1. Have a record of all hardware so you know what your estate looks like
2. Have a record of all software to ensure it is properly patched
3. Utilise secure configuration / hardening guides for all devices
4. Manage data in and out of your network
5. Scan all incoming emails
6. Minimise administrative accounts
7. Regularly back up data and test it can be restored
8. Establish an incident response plan
9. Enforce similar levels of security across the supply chain
10. Ensure suitable security controls in any service agreements (including cloud services)

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-02-17-008-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-219-6
DOI: 10.2824/352617