This is a printable copy for offline review. Completed answers should be uploaded here: https://www.smartsurvey.co.uk/s/5YMEOM/

1. About this exercise

Thank you for participating in our island cyber risk benchmark. We've designed this very carefully to be as quick and easy as possible, and to provide a useful output for your organisation as well as for the Island. The results of this will help guide our work and priorities to keep you, your organisation, and Jersey's community secure.

Further information:

Download the information leaflet

Contact JCSC

Cyber Security Awareness Month 2023

Before you start we've put together a brief FAQ. ***Of course if you don't want to read it right now, feel free to scroll to the bottom of the page and jump in!***

Who is carrying out the survey?
Jersey Cyber Security Centre (CERT.JE) is undertaking this exercise in partnership with the Government of Jersey Digital Economy Team, and supported by our delivery partner Soteria.

Why are you doing this?
Cyber threats have never been more severe. We want to understand where our strengths and weaknesses are as a island so we can can prioritise our resources wisely and make sure we are providing the right support. We also want to give policymakers insight into the risk we carry as a jurisdiction to help them develop informed policies.

Who should respond?
All organisations in Jersey can respond. An IT manager, or the person most responsible for your technology will probably find it easiest to answer.

How long it will take to complete?
It should take 10 to 15 minutes if you have the answers to hand. It may take longer if you need to check with someone else. If there is anything you don't know, you can save the survey and come back to it later.

Why should I do this?
Every organisation has cyber risk. The better we can do our job, the better we can support you - and the less you have to worry about cyber, you can focus on the things that matter to you. We will also be offering a series of drop in sessions where you can talk through your cyber security controls with a JCSC cyber expert who will be able to provide advice and support. These will be completely free - as long as you have completed the survey!

Can I have a copy of the questions to review as a team?
Of course. You can download the questions here for offline review. Having considered your answers, you can then enter them into the survey tool.

Is there a briefing I can share with my board, colleagues, or IT supplier?
There is. You can download a copy of the short 2 page briefing note here.

How did you choose the questions?
The questions are carefully mapped to both the NIST cybersecurity framework and CyberEssentials. They cover all NIST and CyberEssentials controls with the fewest questions possible.

Will you provide personalised feedback?
Yes, once the exercise is complete you will be able to request both your own answers and the benchmark results for comparison. We are also offering free 1:1 review sessions with a JCSC expert during Cyber Security Awareness Month. We'll send you a booking link when we receive your completed survey, or you can book directly here.

How will my data be used?
We will use your data statistically to provide aggregated and anonymised results we can share with partners and use to prioritise our work (for example, we will do more work in the areas people most need help with). If you ask us, we will also go through your individual result with you. We'll use your contact details to contact you about this exercise, and if we need to support you with a cyber incident. We will not share your individual results with anyone else. You can find our more in our privacy policy.

Who will have access to my data?
Only team members who are working on the analysis, or supporting you at your request.

Who is the Data Controller?
Jersey Cyber Security Centre, Department for the Economy. JCSC is registered as a data controller under the Data Protection Law.

Will there be any follow-up?
We will review the outcome of the survey and the success of the exercise to learn and improve. We may then contact you with clarification questions or for next year's benchmark, but what you tell us is up to you.

How can I stay up to date with the results of the exercise and with JCSC?
You can sign up for our monthly newsletter here.

Help! I have a question.
Please email hello@cert.je or call 01534 500 050 and one of the team (Matt, James, Paul, Morgan & Steph) will be happy to discuss this with you.

Let's get started!

2. About your organisation

1. Your name *

2. Name of your organisation *

3. Your position / role *

4. Your email address *

5. Website address

6. Industry / Sector *

7. Turnover: *

- [ ] less than £5 Million
- [ ] between £5 Million and £20 Million
- [ ] more than £20 Million

8. Size *

- [ ] 10 people or fewer
- [ ] 11 to 50 people
- [ ] more than 50 people

3. Instructions

The next few pages ask you about the controls you operate in your organisation.

What do I need to know?

The questions ask about your controls posture

The questions are aligned to the CyberEssentials and NIST frameworks (you may use these already).

There are only a small number of questions, and all have multiple choice answers.

The benchmark is designed to be as easy as possible to complete, but you can contact us if you get stuck on anything.

If you do not know all the answers, you can ask your IT specialist or provider.

You can save your survey and come back to it later if you need to do so.

How do I answer the questions?

'**Yes**' means the control is fully implemented and operates all the time, across all of your business where it applies. It's documented and you know about any exceptions.
(For example you routinely apply software updates on all systems using autoupdate, and you check that this is working)

'**Partly**' means the control is in largely place, but not everywhere it should be, or not all the time, or you are not sure how effective it is. The control may be formal (documented) or informal.
(For example you routinely apply software updates on your main systems using Windows autoupdate, but have an old internet router you've not looked at for a long time)

'**No**' means you do not have the control, or the control is not effective, or you do not know if it is operational.
(For example you routinely apply software updates, but also run unsupported software for which no patches are available)

If you are not sure, provide the best answer you can.

4. Identify

9. Do you have a written record or inventory of the IT systems you use?

An inventory does not have to be complicated. There are software solutions (including free ones) that can do this for you, or you can have a list in a document or spreadsheet. The list should include software, hardware such as servers and network devices, and cloud services such as websites. Your IT provider may maintain this list for you, or you may do it yourself.

---

*

- [ ] Yes
- [ ] Partly
- [ ] No

10. Do you have a record of the data and information assets you hold?

If you are registered under the Data Protection Law you will almost certainly have a record of the data you process, so you may want to check this if you are not sure. This will include information such as employee, customer or user/beneficiary data, and will include email, applications and databases as well as back-ups. Maintaining a record of data assets does not have to be complicated and can be in a simple document or spreadsheet.

---

*

- [ ] Yes
- [ ] Partly
- [ ] No

5. Protect

11. Do you use firewalls to separate your internal network and systems from external networks (such as the internet), and use software firewalls and laptops, desktops and servers?

Firewall is the generic name for a piece of software or a hardware device which provides technical protection between your network devices and the Internet, referred to in the question set as boundary firewalls. Your organisation will have physical, virtual or software firewalls at your internet boundaries. Software firewalls are included within all major operating systems for laptops, desktops and servers and need to be configured to meet compliance. Firewalls are powerful devices, which need to be configured correctly to provide effective security. More information: https://iasme.co.uk/articles/firewalls/

---

*

- [ ] Yes
- [ ] Partly
- [ ] No

12. Do you have a process to securely configure your systems and cloud services to disable unnecessary services, ports, accounts and applications, change default passwords and set secure ones?

Computers and cloud services are often not secure upon default installation or setup. An 'out-of-the box' set-up can often include an administrative account with a standard, publicly known default password, one or more unnecessary user accounts enabled (sometimes with special access privileges) and pre-installed but unnecessary applications or services. All of these present security risks. More information: https://iasme.co.uk/articles/secure-configuration/

---

*

- [ ] Yes
- [ ] Partly
- [ ] No

13. Do you have technical controls to automatically lock user devices when they are not in use, for example when people step away from their desk?

If a device requires a user's physical presence to access a device's services (such as logging on to a laptop or unlocking a mobile phone), a credential such as a biometric, password or PIN must be in place before a user can gain access to the services. You must protect your chosen authentication method (which can be biometric authentication, password or PIN) against brute-force attacks, for example by locking an account after 5 unsuccessful password attempts. *

- [ ] Yes
- [ ] Partly
- [ ] No

14. Do you have a process to regularly update all software and devices (including network devices such as broadband routers and firewalls, mobile phones, websites and cloud hosted services), including patching for security vulnerabilities within 14 days of a patch being released?

Any device that runs software can contain security flaws, known as vulnerabilities. Vulnerabilities are regularly discovered in all sorts of software. Once discovered, malicious individuals or groups move quickly to misuse (or 'exploit') vulnerabilities to attack computers and networks. All such software must be regularly updated and maintained in a supported condition.

If you have a process but take longer than 14 days to apply security patches, or patch most systems but not all, select 'partly'. If you operate any software or devices which are no longer supported by the vendor and cannot be patched, and these are not segregated from the rest of your network, select 'no'.

***

- [ ] Yes
- [ ] Partly
- [ ] No

15. Does every person with access to your network, applications or systems (including your employees, IT team / provider, customers and suppliers) have a unique, individual user account that gives them only the access they need to perform their role?

User accounts should be assigned to individual users and not shared. Passwords and other authentication credentials should be unique to the user and the application. Each account should provide access only to the applications, computers and networks the user needs to carry out their role, and there should be a process for reviewing and removing access promptly when it is no longer required.

*

- [ ] Yes
- [ ] Partly
- [ ] No

16. Do you restrict access to administrative accounts and keep these credentials secure, so they are only used where absolutely necessary?

Compared to normal user accounts, accounts with special access privileges have enhanced access to devices, applications and information. If these accounts are compromised, an attacker could take advantage of their greater accesses to corrupt information on a large scale, disrupt business processes or gain unauthorised access to other devices in the organisation.

Admin accounts in particular can provide very powerful access to access information, change systems settings, create accounts or install applications. These should be separately controlled and restricted. Users should not have 'local admin' access to their computers, and all admin credentials should be stored in a highly protected space such as a good password manager. This also applies to devices such as internet routers and firewalls, as well as externally hosted systems (such as websites). Default admin accounts should be disabled. Passwords should be complex and must not be written down insecurely, and accounts should be protected with multi-factor authentication.

---

*

- [ ] Yes
- [ ] Partly
- [ ] No

17. Do you use strong and unique passwords for all systems, and use Multi Factor Authentication (MFA) for user and admin accounts, as well as all systems accessible from outside your network?

Strong passwords should be generated using a random password generator or a suitable method such as NCSC's three random words. Passwords must be unique, i.e. they should not be used for more than one user, system, application or website. Two Factor Authentication (2FA, also called 2SV) should be implemented on all network accounts as well as all accounts accessible from outside [question(20061548)]'s network, for example email, third party websites, client portals and social media. Passwords should be stored in a secure password manager and not written down insecurely.

---

*

- [ ] Yes
- [ ] Partly
- [ ] No

18. Do you protect your systems from unauthorised and undesirable software by running anti-malware software and/or restricting the applications that can be installed to a pre-approved list?

If a system is infected, your organisation is likely to suffer from problems like malfunctioning systems, data loss, or onward infection that goes unseen until it causes harm elsewhere. You can largely avoid the potential for harm by preventing malware from being delivered to devices, and preventing malware from running on devices. Anti-malware software is available for many operating systems and should be prevent malware from running, prevent execution of malicious code, and prevent connections to malicious websites. It should be updated regularly and users should be prevented from disabling it.

Application allow listing is a technical control to restrict the applications that are allowed to specific signed applications, based on an approved list. This is very effective when done well but can be harder in smaller organisations. A 'soft' version of this is to maintain a list of software you permit, restrict uses from installing new software themselves, and regularly check for anything unauthorised.

---

*

- [ ] Yes
- [ ] Partly
- [ ] No

6. Detect

19. Do you monitor your systems to detect unexpected events (other then system downtime)?

There are many different way of monitoring systems, and this does not always need to be 24x7. Monitoring should include system interruption (such as a server or website failure) and security monitoring (such as for unauthorised access, cyber attacks, outstanding patches, or malware). Monitoring should be appropriate to [question(20061548)] and your risks and needs. If you have a managed IT or cyber security service your provider may do this for you.

Note: Jersey Cyber Security Centre's Cyber Shield can provide additional protection by monitoring for *externally* visible problems on your behalf, and you can sign up here free of charge. However we cannot see what is happening *inside* your network.

---

*

- [ ] Yes
- [ ] Partly
- [ ] No

20. Do you have a process for alerting [question(20061548)]'s IT team or provider of unusual activity on your website, systems and networks so that you can investigate these promptly? This could be in house or via a supplier.

Once you are monitoring your network (or receiving alerts from an IT provider, JCSC's Cyber Shield or UK NCSC's Active Cyber Defence) you will need a way to take action when something is wrong. A process can be as simple as emailing alerts to an IT Manager, service desk, duty manager or external provider, as long as they are able to take action to fix the problem. If you have a managed IT or cyber security service your provider may do this for you.

---

*

- [ ] Yes
- [ ] Partly
- [ ] No

7. Respond

21. Do you have a documented and up to date incident response plan in the event that your cybersecurity is compromised?

Everyone needs an incident response plan. This works exactly like a fire evacuation - when the alarm goes off you already know what you need to do, and have practiced so there are no surprises. Plans do not need to be complicated. They should be documented, reviewed at least annually, and provide enough information that someone who is not an expert on your company could follow it. This would include information on key contacts, service providers, systems, backups, and priorities, as well as how you would contact your customers.

Note: If you need help with your plan, please contact us or sign up to attend one of our incident response workshops in Cyber Security Awareness Month here. Events are open to all.

---

*

- [ ] Yes
- [ ] Partly
- [ ] No

22. Do you test your incident response plan at least annually?

Just as with any emergency plan, it needs to be tested to make sure it will work and everyone knows what they need to do. You can do this yourself or through a provider. Your test should include simulating a cyber attack or system failure, and walking through each step of your plan including restoring systems and data.

Note: If you need help with this, JCSC provide free workshops to help you learn how to do this, and UK NCSC have a downloadable toolkit.

---

*

- [ ] Yes
- [ ] Partly
- [ ] No

8. Recover

23. Have you identified the impact of downtime on your ability to serve your customers, and prioritised your IT systems for recovery?

In an emergency situation you can rarely do everything at once. Listing out your services and systems and agreeing how long you can afford to operate without them helps you understand the consequences of a cyber incident, prioritise in an emergency, and communicate to your customers. For example if you are a retailer, you may be fine for a week without payroll, but only an hour without card payments. Sometimes called an 'RTO' or recovery time objective, targets for recovery should be agreed with your IT team or provider if you have one.

---

*

- [ ] Yes
- [ ] Partly
- [ ] No

24. Do you maintain segregated off-network backups (for both business data and systems configuration), and tested your ability to restore and operate from these?

If your systems are compromised you will need to restore them, and you will only be able to do this if you have a clean, safe copy of your data. This backup should not ne accessible using the same usernames and passwords as the rest of your network, or stored in the same place, or it will be compromised too. Very few organisations that do not have good backups can survive a cyber attack, so it is important to do a test and make sure you can restore if you need too.

---

*

- [ ] Yes
- [ ] Partly
- [ ] No

9. And finally!

25. What independent assurance tests does [question(20061548)] regularly undertake to confirm your cyber security controls are effective?

Some small organisations may have no cyber assurance and others will have a lot. This will depend on your business and also your customers. If you don't have any of these, just select the bottom option - none / don't know.

Government of Jersey mandates CyberEssentials for their suppliers, and Jersey Cyber Security Centre recommends at least Cyber Essentials Plus. These are suitable for all businesses. Larger businesses, or those with more risk, will often also have other assurance.

Note: to find out more about Cyber Essentials, you can attend JCSC's breakfast briefing in Cyber Security Awareness Month.

---

*

- [ ] CyberEssentials
- [ ] CyberEssentials Plus
- [ ] ISO27001
- [ ] Internal Audit
- [ ] Automated Vulnerability Scanning
- [ ] Network Penetration Test
- [ ] Website Penetration Test
- [ ] ISAE3402 / SOC2
- [ ] None of the above / Don't know

Other (please state)

26. How confident do you feel that you have implemented the right controls in [question(20061548)], and would be able to defend against and recover effectively from a cyber attack? *

My confidence level:

Are there any other comments or observations you would like to share?