How to write a **Cyber Strategy**

GATHER
TECHNOLOGY

Simon Hebditch
FOUNDER

How to Write a Cyber Strategy

This document is intended to walk you through the process of writing a Cyber Strategy.

To make this easier, I will use an example business and provide explanations of each section. The example business is called **Care Ltd**, they provide home care services in a rural location and have approximately 100 employees across five different sites. A lot of their employees work remotely, as they visit their clients in their own homes.

Care Ltd are a good business example for this document because:

- Health and social care is a highly regulated sector. The majority of the data they process is extremely sensitive and protected under the duty of patient confidentiality.
- To ensure people are receiving the correct care, health and social care professionals often need quick and remote access to their highly sensitive data.
- Many health and social care providers work collaboratively with other services and share sensitive information. A breach could become disastrous if it extends into this larger network.
- As they strive to improve patient care and innovate through technology, the health and social care sector has become increasingly targeted by criminals and cyber threat actors looking to exploit vulnerabilities.
- Cyber attacks in care have ramifications beyond financial loss and violation of privacy: A cyber breach could be ruinous, not only for their reputation but also in their CQC regulatory reports.

This Cyber Strategy is principally based on the NIST (National Institute of Standards and Technology) Cybersecurity Framework.

As such, our Cyber Strategy will be broken down into the following sections:

- Introduction
- The Cyber Security Environment
- Update on previous year
- Identify and Manage
- Protect
- Detect
- Respond
- Recover
- Action Plan
- Summary

Using the above NIST Cyber Strategy framework, each section in this document will provide an example for the hypothetical business, Care Ltd, followed by a detailed explanation of the section. The aim is to help you understand the logic behind the presented example when you are writing your own.

Introduction

Care Ltd's mission is to provide the very best care and support to people in their own homes. Through our values of innovation in care and putting people first, our vision is to be the home care provider of choice.

We recognise that technology can improve the quality of the care and support that we provide to our clients. By enabling faster and more efficient information sharing, our clients benefit from a seamless integration in their care pathway without the need to repeat their care history to multiple clinicians.

However, as Care Ltd utilises technology more, we must continue to take the best cyber security measures to ensure we are keeping people's information safe and secure. To do this, it is critical that Care Ltd's information systems, which hold a significant amount of highly sensitive data, are protected from the ever-increasing threat of cyber-attacks. The purpose of this document is to outline Care Ltd's Cyber Strategy for 2021-2022.

Our Cyber Strategy is aligned with two main principles of Care Ltd's approach to risk:

- To minimise and manage the impact of risks that could undermine Care Ltd's ability to provide vital care services to our customers.
- To take informed risks, that allow us to innovate and improve the service that we provide to our clients.

This Cyber Strategy outlines the approach and actions Care Ltd will take to address current and emerging risks, with the ultimate aims of preventing cyber attacks and improving our ability to recover from them, should they occur.

Explanation

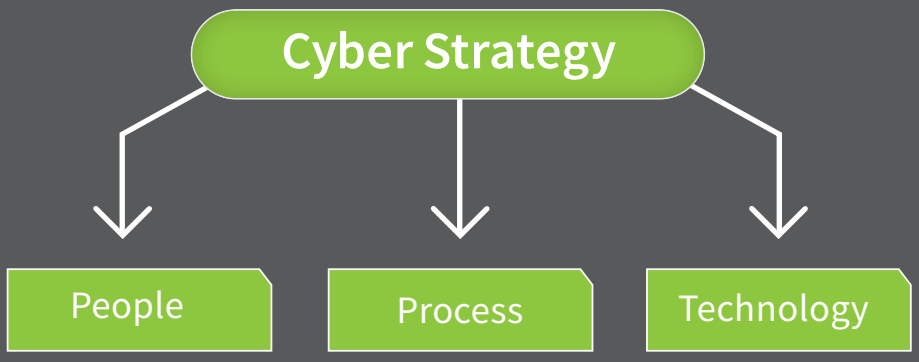
The introduction does not need to do much beyond setting the scene and purpose of the document, as well as some very high level objectives.

What are the very high level intended outcomes that the Cyber Strategy will deliver?

It might help you to write this section if you can answer the following questions for yourself and your business:

1. Why is Cyber Strategy important to you and your business?
2. What is your appetite for risk in general?

> **Your Cyber Strategy will help to inform and guide your decision making. It can be looked at as the very first part of the Cyber Security process:**



It will be referred back to, for example, when reviewing the process for vendor risk assessments to ensure the process is in line with the strategy.

The same is true when considering new technology, or new hires and skills requirements. It is the very first part of the process and must be understood and endorsed at the highest level.

The Cyber Security Environment

2020 saw an unprecedented, enforced move to remote working for a huge number of businesses in the UK and around the world due to the Covid-19 pandemic.

The urgent need for remote working meant that for some businesses, productivity and ease of use were prioritised over security. Cyber Criminals were all too aware that this was the case, and the result was a huge increase in attacks, most notably phishing scams.

This trend shows no signs of abating and increasingly, the threat to information systems is not technology being attacked but people. Social engineering is not new, but every successful attack emboldens those responsible.

The early part of 2021 has seen one of the largest mass attacks ever with the zero-day Hafnium exploit causing mass outages across multiple versions of Microsoft's Exchange Server. It is rumoured that this was a state sponsored attack. A frightening prospect if accurate.

The UK Government's 2021 Cyber Security Breaches Survey has recently been published with one statistic that stands out: In 2020, 65% of medium sized businesses surveyed reported having a cyber attack or breach. 83% of these were reportedly phishing scams, the most of all common of cyber crimes.

Explanation

This section aims to summarise the current threat for readers who may or may not be familiar with what is going on in the world of cyber security. It should be factual and provide some statistics – the government's cyber security breaches survey (link below) contains a wide range of useful information on the subject.

www.gov.uk/government/collections/cyber-security-breaches-survey

It would be my recommendation that the facts you include are as specific as they can be to your organisation.

Update

Since Care Ltd began our Cyber Security initiative, all IT systems and data security protocols have been designed around the highest standard of patient care and the needs of front line staff. This removes the necessity for our staff to create workarounds, which introduces risk into Care Ltd's systems.

Care Ltd has replaced or reduced hardware and software that can no longer be supported. We have invested in better cyber security expertise for monitoring, threat intelligence and incident responses.

All members of Care Ltd now understand the importance of cyber security and the nature of the growing cyber risk. We have actively empowered our staff to improve their cyber awareness through inclusive training on best practices. We will continue to drive cultural change at all levels of our organisation.

As part of our ongoing cyber strategy, Care Ltd delivered the following improvements to protect its information systems in 2020

- Implemented a secure remote access solution utilising next generation technology powered by Citrix.
- Further secured our email with Mimecast email filtering.
- Significantly improved our users' Cyber Security Awareness by implementing a training solution called Cybsafe.

In 2020, Care Ltd suffered several attempted cyber-attacks and phishing attempts but thankfully, none were successful and there were no breaches.

Explanation

The update is here to give the reader an overview of what has happened in the previous year, in particular referencing last year's strategy document if it exists. Be sure to include the progress made in your cyber strategy and, critically, any areas of improvement. This is also a good point to cover any incidents or breaches from the previous year, albeit at a very high level.

The theory behind this section is to continue setting the scene for the rest of the document.

Identify and Manage

Care Ltd cannot be complacent. The cyber threat is growing and constantly evolving. It requires continued vigilance and a collective effort across all of Care Ltd's operations, including our vendors and suppliers.

Care Ltd will ensure that it has the people, processes, and technology in place to identify and manage Cyber Security Risk.

Intended Outcomes

- Care Ltd will have access to people with the right skills to assess and advise on Cyber Security.
- Roles and responsibilities for the delivery of the Cyber Strategy will be clearly defined.
- Governance of processes and policies will be robust and straightforward.
- Cyber Risk Management will be incorporated into the decision-making process at every level.
- All information systems are clearly identified and understood.

Strategic Initiatives

- Annual third-party Cyber Risk Assessment.
- Rigorous vendor risk assessment process.
- Improved reporting metrics around Cyber Risk to inform senior management decision making.

Explanation

Identifying and Managing Cyber Risk is the objective of this section.
It should consider the following areas:

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management

These are all in depth subjects in and of themselves, the primary aim of this section within the context of a cyber strategy is simply to outline the very high-level considerations, requirements, and goals.

Protect

As a home care provider, we have a duty to identify and protect all of Care Ltd's data, most notably any personal data belonging to our clients. As we work closely and share information with other health and social care services, we must also uphold a professional responsibility to demonstrate that we are following best practice to meet legal and regulatory requirements.

We recognise that all health information is extremely sensitive and our cyber security protocols must ensure that Care Ltd's data is protected with all potential risks minimised. As custodians of our clients' data, it is imperative for the ongoing success of Care Ltd that we take appropriate steps to secure and protect this data. Any cyber breaches and security threats will have a direct impact on our clients and, therefore, our quality of care.

Intended Outcomes

- All staff can identify and classify sensitive data in accordance with Care Ltd's processes and policies.
- Access to information systems is strictly controlled and granted only by authorised personnel.
- Best of breed technology protects our mission-critical information assets.
- Cyber Security Awareness among our staff exceeds our competitors.

Strategic Initiatives
To achieve these intended outcomes, Care Ltd will:

- Continuously monitor and improve the cyber security awareness program.
- Enhance and develop processes and tools to categorise sensitive data.
- Implement technology-based solutions to detect and prevent data loss.
- Create KPIs that report on Cyber Security Awareness and contribute to the overall Cyber Risk metrics.
- Complete the Cyber Essentials Plus certification.

Explanation

The Protect section of a Cyber Strategy should demonstrate your commitment to, and plans for, protecting the data that you hold. It should also recognise any particularly sensitive data that needs special consideration. The intended outcomes should outline what you need to do to protect this information. Areas of consideration are:

- Identity Management and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

Some of these areas may be more or less relevant to you and your business but it is important that you are conscious of them all as you write this section.

Detect

Our cyber strategy not only promotes learning to develop company-wide cyber security awareness and understanding, we also actively encourage an incident reporting culture. Through continued education and technological expertise, Care Ltd is committed to having cyber defence capabilities that will find a problem when it does occur.

Intended Outcomes

- Cyber-attacks are rapidly detected using intrusion detection systems.
- The attack surface is minimised by the consistent monitoring of security configurations.
- Our understanding of the threat landscape is well-informed by timely threat intelligence.

Strategic Initiatives

To achieve these intended outcomes, Care Ltd will:

- Conduct regular cyber security tests to exercise cyber defences, detection, and assessment capabilities.
- Ensure that it has strong standards and processes in place for security configuration and continuously monitor for configuration changes.
- Our understanding of the threat landscape is well-informed by timely threat intelligence.
- Measure and improve the processes used to handle threat intelligence.
- Implement next generation security monitoring tools and processes, such as expanded end-point detection and managed security operations centre with 24 x 7 always on threat detection in real time.

Explanation

This section should outline what is required for your business to detect and manage cyber-attacks. There is little value in being too specific, that will come later, rather, focus on the more general goals and tools that you will be employing.

Consider:

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

This section is more technical than the others as it is quite specific about how your business will detect Cyber Attacks. It might be that very little here applies to you and that you rely upon human detection, rather than technology solutions. If this is in line with your risk appetite, then that is not a problem but it's important to be honest with yourself and your business.

Respond

We acknowledge that despite our best efforts, a Cyber Incident could still happen at Care Ltd. To limit the impact of any potential cyber security incidents, we will outline immediate actions and follow-up procedures. These steps will be shared with our entire organisation, so everyone can react and respond effectively if/when an incident occurs.

Intended Outcomes

- A Cyber Security Incident Response Team with all of the skills necessary to manage and minimise the impact of a cyber security incident.
- Processes and procedures to effectively coordinate response activities with internal and external stakeholders.
- Processes and controls that meet the standards required by regulators.
- Appropriate forensic investigation capabilities that ensures forensic investigations can be conducted without delay and with the required information.

Strategic Initiatives

To achieve these intended outcomes, Care Ltd will:

- Continue to train and invest in the people upon which it relies to manage cyber security incidents.
- Perform cyber security tests to exercise the effectiveness of the incident response process, using the results to contribute to the overall Cyber Risk metrics.
- Seek and retain the services of cyber forensic and technical experts.

Explanation

It's important to understand and acknowledge that it is impossible to completely prevent cyber incidents. The biggest companies in the world spend millions, possibly billions on trying to do so and yet almost weekly in the news, something has happened. And those are only the incidents that make it to mainstream media. Imagine the number that doesn't get reported…

With that in mind, the Respond section demonstrates that your business is prepared for the worst-case scenario, should it happen.

You should think about:

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Respond dovetails with Recover to inform your plans for dealing with a Cyber Attack. They are closely linked and so should be handled in close coordination with one another, rather than technology solutions.

Recover

At Care Ltd, we have several mission-critical systems with highly sensitive information. Fast recovery from any cyber breach is essential: Not only to ensure our staff has access to the correct client files but also as we share information across external health and social care networks.

Care Ltd will ensure that it can recover from a cyber incident and restore normal business operations in a timely fashion.

Intended Outcomes

- Mean time to recovery (MTTR) from a cyber incident is in line with business requirements.
- Tested and proven recovery plans are in place for all mission-critical systems.

Strategic Initiatives

To achieve these intended outcomes, Care Ltd will:

- Practice and rehearse specific cyber incident scenarios, in particular, the ability to recover from a ransomware attack.
- Measure the MTTR and report on it to contribute to the overall Cyber Risk metrics.

Explanation

The recovery section is relatively self-explanatory – its principal aim is to show that you have thought about how you will recover from a cyber incident were it to occur.

This section ties in closely to the respond section – disaster recovery and business continuity planning and are likely to overlap the outcomes and initiatives of both of these sections, as do the areas that you need to consider:

Consider:

- Response Planning
- Improvements
- Communications

In the same way that disaster recovery planning was the hot topic 15 years ago, so cyber security incident planning is the hot topic today.

Test your plans!

Failing to prepare is preparing to fail and it is well worth spending the time to think about and plan what you would do if you suffered a breach.

Action Plan

At Care Ltd, we recognise and acknowledge that a strategy without an action plan has little value.

In developing our action plan, we have utilised the expertise of our industry regulators and technology specialists. We have taken into account all changes flagged up during a recent cyber security audit.

We also actively engaged and listened to our service users, care professionals, support staff, operational managers and board members to ensure a unified and comprehensive resolution.

Our Cyber Strategy Action plan has been clearly documented, stored centrally and widely distributed so that every member of our organisation has access to it.

On the following page, we outline the procedures and practices that will help us deliver our Cyber Strategy.

Explanation

This section will cover the activities, plans and if appropriate, time lines associated with them.

It will cover additions and improvements, not maintenance activities. For example, there is no need to put in here the name of each policy document that will be reviewed however, if it has specifically been identified that the Information Sensitivity Policy Document will be rewritten, that could and should be included.

Some of these actions might be very high level at this stage but that is to be expected, the important thing is to demonstrate and direct the attention of the business to the areas that require action to deliver the cyber strategy.

Remember, the cyber strategy should probably not involve technical staff at the stage of its conception but, once it is written, it can be used to create initiatives and inform discussions with them over projects and activities for the coming time frame.

Your action plan should be included in the cyber strategy, but it is also useful to store it as a separate document. This way it can be distributed across your organisation more easily. The more employees who are aware and engaged with the process, the more people who can protect your business.

OBJECTIVE	IDENTIFY & MANAGE	PROTECT
Activities Roadmap 2021 - 2022	Engage third party to perform a cyber security risk assessment.	Include cyber security awareness training in performance reviews.
	Create and enforce vendor risk assessment process.	Review and report on technology solutions for simple data classification.
	Create a Cyber Risk metrics dashboard that is easily accessible and aids decision making.	Include cyber security awareness KPIs in the Cyber Risk metrics dashboard.
		Source and implement data loss prevention technology solution.
		Complete Cyber Essentials Plus certification.

DETECT	RESPOND	RECOVER
Engage third party to perform quarterly cyber security tests.	Investigate and review CISSP and other equivalent qualifications and report on if the business should seek to have such a resource in house.	Perform a full recovery of the most sensitive data, as though it were lost as part of a ransomware attack.
Implement technology solution to monitor and enforce security configurations.	Create KPIs to report on the effectiveness of the cyber security incident response process, in line with cyber security tests.	Measure the MTTR as a part of the above recovery and ensure that it is in line with our requirements. Report on it as a KPI.
Create KPIs around the handling of threat intelligence so that the process can be measured and improved.	Engage with third parties to quote for a managed cyber security service, this could be as part of the 24 x 7 SOC.	
Engage third parties to quote for 24 x 7 Security Operations Centre.		

Summary

As health and social care changes with technological advances, so to must we adapt and respond to its shifting landscape, whilst adhering to our core mission of providing the highest standard of person-centred care.

When it comes to cyber security, our goal is to minimise risk to maximise our service. Our Cyber Strategy for 2021-2022 showcases our understanding that cyber security continues to represent a serious threat, but also an opportunity for growth. By developing excellent IT security governance and a reliable, efficient IT infrastructure, more time is released for our employees to spend on quality-driven care.

Care Ltd will strive to incorporate this philosophy into every area of our business to ensure it becomes a core part of our culture.

Our ambition is to be ahead of our competitors in every regard, our cyber security strategy is no different. By demonstrating that we care for our information systems and sensitive data, we are directly caring for our clients and continuing to enhance our reputation as an outstanding home care provider.

Explanation

Here, we are looking to bring the document to a close by summarising why we have written this document and what it will deliver to the business.

This is highly personal and will range in tone from ambitious to conservative – the important point is that it encapsulates and explains your business' position on cyber security.

In Conclusion

Through examples and explanations, this document has demonstrated the processes and logic behind a Cyber Strategy.

Writing your first cyber strategy may seem like a monumental task, but it is critical to a robust approach to cyber security. Although Care Ltd's Cyber Strategy is hypothetical, the cyber threat is very real and growing daily. A cyber attack or social engineering scam is inevitable, but a breach could be avoided through preparation and awareness.

Our final points for you to consider whilst creating your cyber strategy:

Prioritise Based on Risk

What is high risk and needs to change immediately? What is ongoing or requires cultural change?

Key Staff & Cyber Awareness

Who are your key members in your strategy? Have you considered the cyber skill sets and security training of all your employees?

Business Continuity

What does your business need to keep running IF there is a breach? What systems are vital?

Policies & Procedure

Who is responsible for updating policies and aligning them with your business' procedures?

Communication & Response

What happens if things do go down and your team needs to keep working? Do you need to share details of a breach with clients?

Monitoring & Audits

Have you got a good IT partner? Do they provide ongoing monitoring, IT updates and annual audits?

I hope the hypothetical examples and explanations provided have been useful in writing your own cyber strategy. If you'd like further help with your first cyber strategy or an expert eye over your current one, please get in touch for a no-obligations chat.

Book an initial chat

GATHER
TECHNOLOGY