GUIDANCE

Cyber Security Toolkit for Boards

Resources to help Boards implement the actions outlined in the Cyber Governance Code of Practice.

Pages

Cyber Security Toolkit for Boards

Introduction +

Principle A: Risk Management +

Principle B: Strategy +

Principle C: People +

Principle D: Incident Planning, Response and Recovery −

Planning your response to cyber incidents

Principle E: Assurance and Oversight +

Resources +

PUBLISHED

30 March 2023

REVIEWED

8 April 2025

VERSION

3.0

WRITTEN FOR

Large organisations

Small & medium sized organisations

Public sector

Cyber security professionals

Was this article helpful?

Yes No

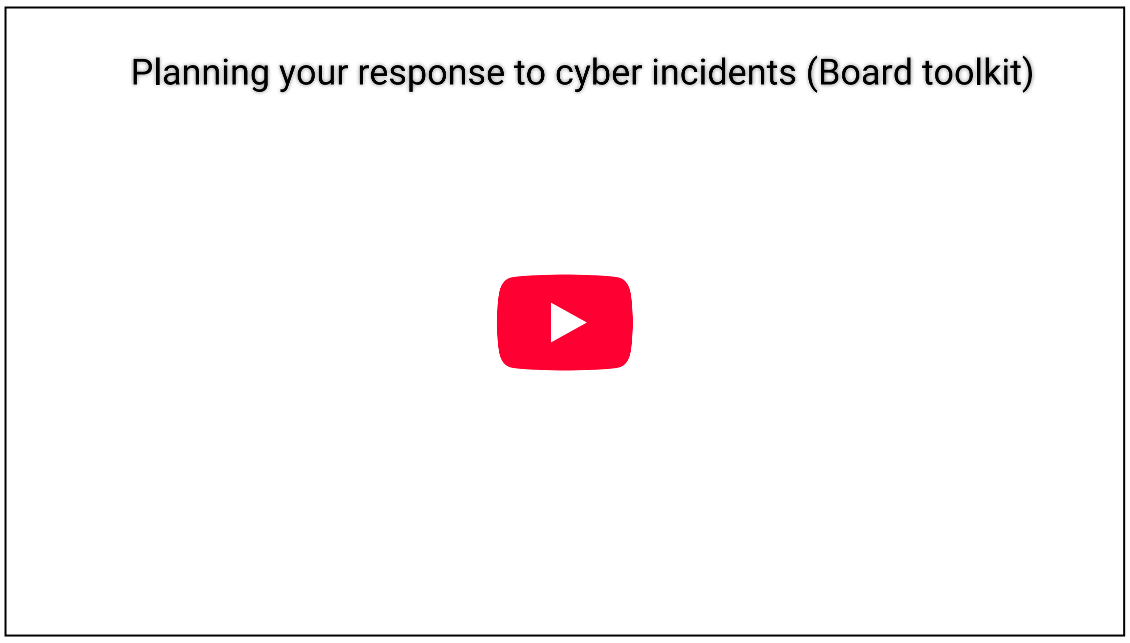
PAGE 16 OF 27

Planning your response to cyber incidents

ON THIS PAGE

1. Introduction
2. Essential activities
3. Indicators of success

Good incident management can reduce their financial, reputational and operational impact.



Planning your response to cyber incidents (Board toolkit)

Introduction

Cyber security incidents (such as a data breach or ransomware infection) can have a huge impact on an organisation in terms of cost, productivity, reputation and loss of customers. Being prepared to detect and quickly respond to incidents will prevent the attacker from inflicting further damage, and can reduce the financial and operational impact.

During an incident, it's imperative the board remains operationally focussed. Handling the incident effectively whilst in the media spotlight will help to reduce the impact on your reputation and loss of customers.

Having a well-prepared cyber incident response approach is essential for cyber resilience. The benefits include:

- Key decisions and considerations can be planned in a less stressful environment and their implications properly understood
- business is restored more quickly, minimising financial losses
- legal obligations are complied with early and openly
- prompt and decisive action restores public confidence and trust, and reassures shareholders
- clear communication will alleviate fears and anxiety in the workforce
- learning from the incident and strengthening security will better prepare the organisation for future incidents

Ransomware attack on a large industrial business from the eyes of its C level team

What preparation did the organisation have in place before the attack?
The board had agreed the organisation's cyber strategy well in advance of the attack. Our cyber risks had been updated and we had carried out both technical and board-level exercises. Helpfully, we had anticipated ransomware as a potential risk and so it was one of the incidents we'd rehearsed. Underpinning this was business continuity plans across our businesses and a disaster recovery plan to support it. This level of planning undoubtedly helped us in the real event.

What were the first signs of the attack?
Our security operations team experienced an increase in alerts which were indicative of a serious threat to our systems. These were out of the ordinary and conducive to their being an active cyber criminal in the network.

What was the immediate response?

The immediate response was to contain the attack on our network and systems. This alone took more than a week and was like being in a fist fight with a determined cyber criminal. Every action we took to defend our systems was met with a counter-response from the criminals.

What third party organisations did you contact for help/advice?

We engaged with external third party subject matter experts and used relationships we had built within the industry to get externally skilled resources onsite. The NCSC incident team and local law enforcement were also informed. Relationships we had built with other third parties allowed us to spend time speaking with another CEO who had experienced a devastating ransomware attack. This not only provided us with an external perspective on how impactful these types of attacks can be, but their knowledge and experience also provided myself and the board with more insights to help us lead the business out of the crisis.

Were they helpful?

Getting support from outside the organisation played a critical part in our defence and recovery. We had highly skilled internal resources but realised quickly that we would need more support to ensure we could continue defending and recovering the business without burning out our teams.

Did anything change?

We felt the tempo and intensity of the attack increase throughout the week. NCSC confirmed to us during the post-incident forensic analysis that the attack had indeed intensified and that sophisticated and determined cyber criminals were involved.

How was the morale of the team?

The general morale of the team varied as the incident progressed and this is something we had to closely monitor throughout. The team were working hard to tackle what was a particularly complex attack, in a fast-paced and fluid environment. In addition to incident containment, the team also had to address business continuity. This resulted in a stressful time for us all, and many members of the team had to spend time away from home or numerous hours on Teams calls. Where possible we tried to put measures in place to reduce the amount of business continuity tasks teams had to be involved in so they could focus on incident response. The CEO and Chair also helped to boost morale by visiting the team on a number of occasions.

When were comms issued to shareholders and customers?

Our communications strategy was multi-faceted so that we could ensure the interests of a number of different stakeholders (employees, customers, shareholders, suppliers, relevant regulators) were met.

No customer data was compromised, however, we did notify customers where appropriate where it was determined that delivery times would be impacted.

Did you pay the ransomware money?

No. We did not engage with the ransomware attackers at all. We disrupted the attack, and felt that we could recover without having to engage with the cyber criminals. We had confidence in our team and our business that we could recover from the attack on our own terms.

What was the cost to the organisation?

The organisation was impacted through deferred revenue and loss of associated profit, under-recoveries and direct costs associated with incident response, with total financial impact in the year estimated at around £25m.

Did you suffer any reputational damage?

We did not suffer any long-term reputational damage and were able to provide more clarity and information to our stakeholders as time went on. Further details on the status of the attack and updates on the financial impact were provided in our trading updates.

Were there any lessons learned as a result of the attack and has it resulted in positive changes to the organisation?

The positive impact was that we were able to accelerate planned changes to enhance our security, and we benefitted from tailored input from external expertise.

Is there any advice you would give to other organisations regarding planning for or dealing with a ransomware attack?

Use exercises to ensure the basics are being done really well when it comes to key cyber hygiene across areas like patching and access control across your systems. It is also helpful to understand your environment as much as possible (for example, what suppliers you have in your supply chain, how they are connected to your systems, what data they have).

Experiencing an incident?

If you are currently experiencing an incident, you can contact the NCSC.

Essential activities

Plan your response

Ensure your organisation has an incident response plan in place as it will minimise the impact of incidents, helping normal operations to be resumed as quickly as possible. It should be regularly reviewed and maintained to ensure that it continues to be relevant as roles and structure of the organisation changes. The incident response plan must set out:

- how the severity of an incident is determined
- delegation of authority to make key decisions
- responsibilities for contacting key individuals in the organisation (including board members), suppliers and regulators to share information about the incident

Understand your role

The quality of decision making can be compromised in times of crisis, so it is vital that everyone has a clear understanding of their role and the organisational response in advance. Responding to an incident may require making major decisions such as whether to take systems offline (for instance your public facing website, or other operationally critical systems). It is critical that people know what authority they have, especially if an incident happened outside of normal business hours. For more details about essential roles and responsibilities during incidents, please refer to the NCSC’s detailed Incident Management Guidance.

Practise your plan

Exercising your incident response procedures is as important as practicing fire drills. It is no good having a procedure if no-one remembers what it is, or you only discover that part of it doesn’t work when you're in the middle of a real situation.

- Board members involvement in these activities can really help (whether participating as an observer or a 'player' in the scenario) as a rehearsal for what would happen in a real event.
- Exercises can be run in a variety of ways, from 'tabletop' to more in-depth simulations, which are an excellent way of identifying areas of continuous improvement. The NCSC has produced 'Exercise in a box,' a free resource that provides you with a number of scenarios, based on common cyber threats.
- It may be beneficial to involve partners and service operators in the exercise. You should also consider what you would do in the event that a supplier is compromised.

Learn lessons

An incident can provide valuable insight into your cyber readiness. You should ensure your organisation has processes for conducting post-incident analysis. This generates insight that can help you reduce the likelihood of incidents occurring in the future and reduce their potential impact. For this to work you need to be able to be honest and objective about what has happened. Consider rewarding people for being open and contributing insights into what happened. Critically for the board, responsibility for incidents or data breaches sits with the organisation and not an individual. Therefore the board is ultimately responsible for any cyber security incident as the governing body.

Ensure you can spot events

Depending on their motives, an attacker is unlikely to tell you when they have successfully compromised your organisation. So you need your own methods to identify an intruder or an attack. This normally takes the form of monitoring. Monitoring refers to observing data or logs collected from your networks or systems to identify patterns or anomalies that could indicate malicious activity. Even if you don't have monitoring to identify the incident when it happens, it is still useful to collect system or network logs so that you can retrospectively review them once you know an incident has occurred.

36%

of medium and large organisations don't have an incident response plan in place*

If you're one of these organisations, then **you should address this immediately**.

* Cyber security breaches survey 2024:*Formal incident response plans are not widespread only 55% of medium-sized businesses and 73% of large businesses have them.*

Indicators of success

➕ Show all

› Does your organisation have an incident response plan in place, and do you regularly exercise it? + Show

› Does every board member understand what's required during an incident? + Show

› If a significant cyber incident has occurred in the recent past, can the person responsible for cyber security report what improvements have been made? + Show

› Are cyber incidents considered in the design of your Disaster Recovery (DR) and Business Continuity Plans (BCP)? + Show

› As an organisation, do we know where we can go for help in an incident? + Show

Next page →

Principle E: Assurance and Oversight

← Previous page

Principle D: Incident Planning, Response and Recovery

Topics

Cyber strategy | Risk management

PUBLISHED

30 March 2023

REVIEWED

8 April 2025

VERSION

3.0

WRITTEN FOR

Large organisations

Small & medium sized organisations

Public sector

Cyber security professionals

Was this article helpful?

Yes No

Also see

BLOG POST 07 May 2025

Software Code of Practice: building a secure digital future

New voluntary code of practice for technology providers defines a market baseline for cyber...

BLOG POST 08 Apr 2025

New online training helps board members to govern cyber risk

The NCSC's CEO, Richard Horne on the new cyber governance resources giving Boards...

BLOG POST 01 Apr 2025

Cyber Security and Resilience Policy Statement to strengthen regulation of critical sectors

New proposals will combat the growing threat to UK critical national infrastructure (CNI)