CYBER INCIDENTS

ESTD 2023
TEMPLE AVENUE GROUP

The Crucial Role of Coordination

PRESENTED BY

TEMPLE AVENUE GROUP

TEMPLEAVENUEGROUP.COM

ESTD 2023
TEMPLE AVENUE GROUP

Table of Contents

Summary

LESS THAN A THIRD OF LARGE BUSINESSES HAVE A CYBER INCIDENT RESPONSE PLAN

Coordination plays a critical role in responding to cyber incidents effectively. The increasing complexity and frequency of cyber-attacks, underscores the need for a strategic coordinated response that includes clear communication, executive escalation, and control over the narrative. This helps to prevent a chaotic aftermath of a cyber incident from spiralling out of control.

The financial impact for a cyber breach in the UK services industry is above the norm:

Average cost of a Cyber Incident to a UK Service business stands at £5.2m for 2023, with an estimated cost per victim at £15,300,

With 11% of business having experienced a cyber crime. Yet over a third of large businesses and half of medium sized business do not have an Incident Response Plan.

Coordination of communications is paramount in a cyber incident response. We have outlined a number of steps that organisations can take to improve their client communications, doing so will mitigate the damage to their reputation and bottom line.

With consulting services across Prepare: Manage; Follow-up and Improve- Temple Avenue Group offers a comprehensive cyber management response solution. Employing a programmatic approach, crystal-clear processes, and robust executive escalation mechanisms.
We work closely with your organisation to establish a tailored incident response programme that aligns with your specific needs and risks.

The Crucial Role of Coordination in Cyber Management Response

EFFECTIVE INCIDENT RESPONSE IS INSTRUMENTAL IN REDUCING THE IMPACT OF A CYBER BREACH

In today's digital landscape, where cyber threats loom around every corner, the need for a well-orchestrated and coordinated cyber management response cannot be overstated. The complexity and frequency of cyberattacks demand a strategic approach that encompasses central coordination, clear communication, executive escalation, and unwavering focus on maintaining control over the narrative.

Coordination is the linchpin that holds the entire cyber management response together. When an organisation falls victim to a cyber incident, the chaotic aftermath can quickly spiral out of control without a well-coordinated response. Central coordination involves having a designated incident response team that orchestrates efforts across various departments and functions. This team ensures that actions are synchronized and resources are allocated efficiently. In essence, central coordination acts as the backbone, providing the structure needed to effectively combat a cyber threat.

Financial Impact

$4.45M THE GLOBAL AVERAGE COST OF A DATA BREACH IN 2023

£3.4m

The UK average cost of a data breach in 2023

£5.3m
Financial Services Industry Impact

£5.2m
Services Industry Impact

£4.9m
Technology Industry Impct

Source: IBM Cost of a Data Breach Report 2023

CYBER CRIME

11%
of businesses experienced cyber crime

2,390,000
Estimate instances of UK cyber crime

£15,300
Estimated Average cost per victim

FORMAL INCIDENT RESPONSE PLANS ARE NOT WIDESPREAD

21%
of businesses have them

47%
for medium-sized business

64%
for large businesses

Source: UK Government Cyber security breaches survey 2023 Published 19 April 2023

Communication

THE IMPORTANCE OF A UNITED FRONT

Coordination of communications is paramount in a cyber incident response for several critical reasons. First and foremost, it ensures a unified and consistent message, both internally and externally. In the chaotic aftermath of a cyber incident, misinformation or conflicting information can cause confusion, hampering the organisation's ability to contain and recover from the breach.

Moreover, effective coordination of communications fosters collaboration among various teams involved in the incident response. Cybersecurity incidents often require input from IT, legal, compliance, public relations, and senior management teams, among others. Coordinated communication channels facilitate the exchange of critical information and enable these teams to work in concert towards a common goal, enhancing the organisation's ability to mitigate the impact of the breach, comply with regulatory requirements, and protect its reputation. In a landscape where cyber threats are constantly evolving, the ability to respond swiftly and cohesively is a crucial aspect of an organisation's overall cybersecurity strategy.

Consequently, by centralising communications through a designated incident response team, the organisation can maintain control over the narrative, reduce the risk of panic, and instill confidence among stakeholders.

AFTER A CYBER BREACH

Tips for effective communication

BY TAKING THESE STEPS, ORGANISATIONS CAN IMPROVE THEIR CLIENT COMMUNICATIONS IN THE WAKE OF A CYBER INCIDENT AND MITIGATE THE DAMAGE TO THEIR REPUTATION AND BOTTOM LINE.

BE TRANSPARENT

Don't try to hide anything from your audience. Be honest about what happened and what steps you are taking to address the issue.

BE TIMELY

Don't wait days or weeks to communicate with your clients about a breach. Get the message out as soon as possible.

BE CLEAR & CONCISE

Use plain language that your clients can understand. Avoid using technical jargon or acronyms.

BE EMPATHETIC

Understand that your clients may be concerned about the breach. Acknowledge their concerns and let them know that you are taking the issue seriously.

BE CONSISTENT

Make sure that the communication is consistent across all channels. This will help to ensure that clients are getting the same message

01 CREATE A DEDICATED TEAM

This team should be responsible for communicating with all stakeholders, including clients, employees and partners.

02 ANSWER THE TOUGH QUESTIONS

Clients may have a lot of questions about the cyber incident. Be prepared to answer them honestly and in a way that is easy to understand.

03 UPDATE ON PROGRESS

Keep clients updated on the progress of the investigation. This will help to build trust and confidence.

04 OFFER SUPPORT

Offer support to affected clients. This may include providing credit monitoring or identity theft protection.

05 IMPROVE

Learn from your communications as you go and take the opportunity to improve

ESTD 2023
TEMPLE AVENUE GROUP

Beyond Communication

RAPID EXECUTIVE DECISION MAKING & CLAIRTY

Another vital aspect of coordination is executive escalation. When a significant cyber incident occurs, timely decisions are crucial. The incident response team must have protocols in place to quickly escalate issues to senior management or executives. This ensures that high-stakes decisions can be made promptly, allocating resources and authorising actions to mitigate the impact of the breach. In essence, executive escalation streamlines decision-making, preventing delays that could exacerbate the consequences of a cyber incident.

In conclusion, the importance of coordination in a cyber management response cannot be emphasised enough. Central coordination provides structure and order, ensuring that all efforts are aligned and synchronized. Communication, when centralised, maintains a consistent message and reduces confusion. Executive escalation enables rapid decision-making, and clarity is the antidote to chaos. In the face of evolving cyber threats, organisations that prioritise coordination are better equipped to navigate the tumultuous waters of cybersecurity and emerge stronger on the other side.

Clear and concise communication is the bedrock of any effective coordination effort. Clarity ensures that everyone involved understands their roles, responsibilities, and the current state of the incident. In a high-pressure situation, clarity reduces the potential for misunderstandings or misinterpretations. This means that actions can be executed with precision, and resources can be deployed where they are most needed.

TEMPLE AVNUE GROUP
CYBER MANAGEMENT RESPONSE

COORDINATED

CYBER SERVICES

01 PREPARE:
Develop Incident Management Response Plan

02 MANAGE:
Coordinated Cyber Incident Management Response

03 FOLLOW UP:
Effective close - lessons learned

04 IMPROVE:
Programme Management of Remediation activity

Temple Avenue Group offers a comprehensive cyber management response solution that employs a programmatic approach, crystal-clear processes, and robust executive escalation mechanisms. We work closely with your organisation to establish a tailored incident response programme that aligns with your specific needs and risks.

Central Coordination
Applying programmatic rigour to the centrally co-ordinated approach.

Communication
Clear and timely communication to internal and external stakeholders.

Executive Escalation
Protocols to support informed and rapid executive decision making.

Clarity
Efficient & effective minimising confusion during high-pressure situations.

ESTD 2023
TEMPLE AVENUE GROUP

Questions? Contact us.

ESTD 2023
TEMPLE AVENUE GROUP

www.templeavenuegroup.com
consult@templeavenuegroup.com

MANAGING PARTNER:
Christopher Allix
Christopher.Allix@templeavenuegroup,com