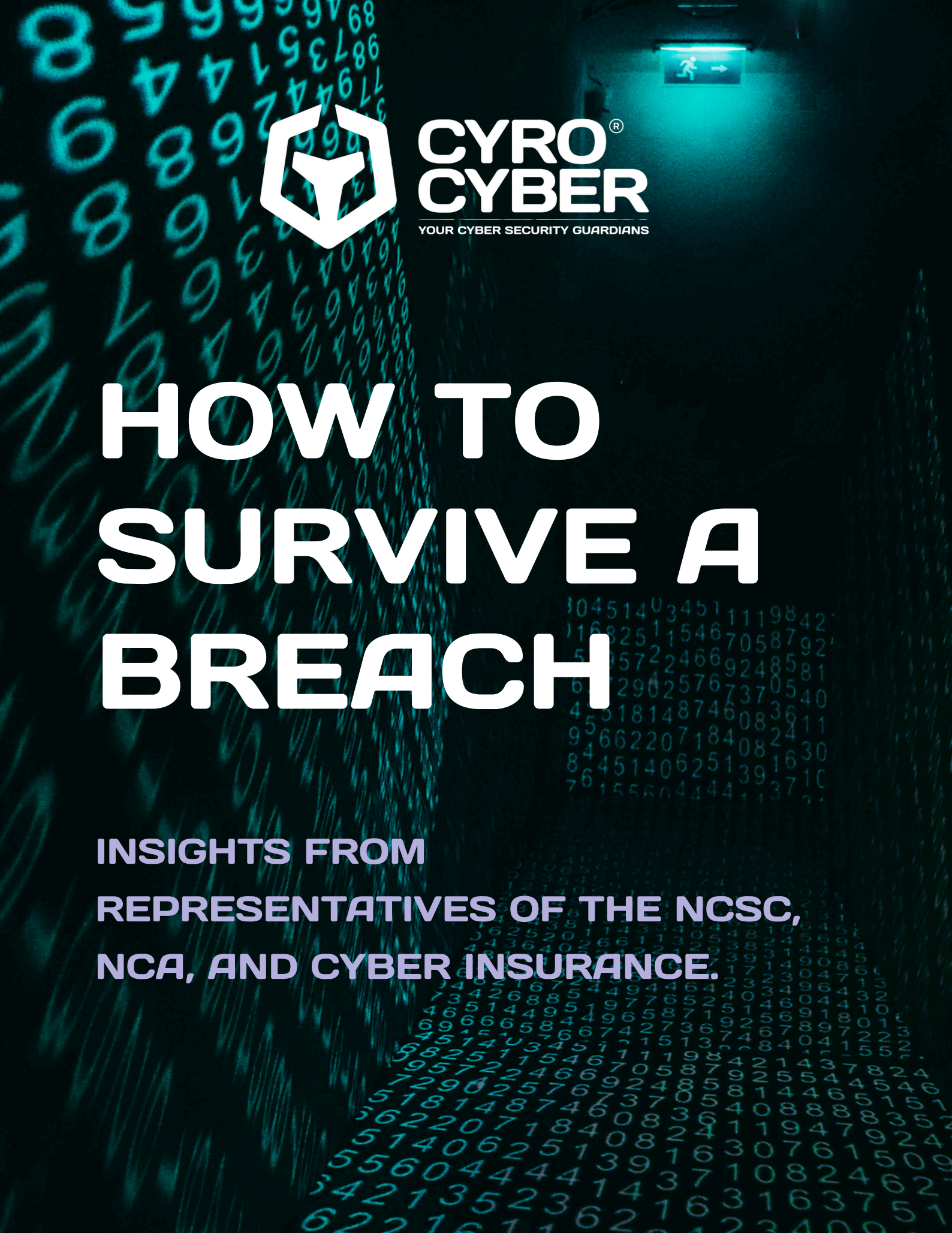

CYRO® CYBER

YOUR CYBER SECURITY GUARDIANS

# HOW TO SURVIVE A BREACH

## INSIGHTS FROM REPRESENTATIVES OF THE NCSC, NCA, AND CYBER INSURANCE.

CYBER ESSENTIALS CERTIFIED PLUS

CYBER ESSENTIALS CERTIFIED

ISO 9001 ISOQAR REGISTERED

ISO 27001 ISOQAR REGISTERED

CREST PEN TEST SOC

Crown Commercial Service Supplier

GovAssure

in association with National Cyber Security Centre

Cyber Resilience Audit

# DISCLAIMER

This report is a summary of discussions held during a Cyro Chapter event featuring representatives from the National Cyber Security Centre (NCSC), the National Crime Agency (NCA), and the cyber insurance sector. It solely captures the insights shared during the session. The views expressed do not necessarily represent the official positions, policies, or full perspectives of Cyro Cyber or the organisations involved.

# ACKNOWLEDGEMENTS

We extend our sincere thanks to our representatives from the NCSC, the NCA, and the cyber insurance sector, whose identities have been redacted to protect their privacy, for sharing their expertise which has shaped the guidance in this report.

# INSIGHTS FROM THE EXPERTS

"We've just been breached" – the words no leader ever wants to hear. Yet for many organisations, they are becoming an unavoidable reality.

More than 40% of UK businesses reported a cyber-attack in the past year, rising to 67% for medium and 74% for large enterprises.[1] It's now commonly accepted that most organisations will experience a breach at some point.

The decisions made in the first moments after a breach will shape how regulators, customers, and the public perceive your organisation for years to come. Public trust, regulatory scrutiny, and operational continuity are all on the line.

At our latest Cyro Chapter, representatives from the NCSC, the NCA, and the cyber insurance sector shared their experiences from the front lines of incident response. This report distils their advice on this topic into lessons you can apply today.

[1] Department for Science, Innovation & Technology. Cyber Security Breaches Survey 2025

# THE CURRENT THREAT LANDSCAPE

**"BROADLY SPEAKING, MOST ATTACKS WE SEE ARE RELATIVELY UNSOPHISTICATED BUT VERY EFFECTIVE. THE BARRIER TO ENTRY FOR ATTACKERS IS LOWER THAN EVER."**

Many organisations assume that cyber criminals use highly sophisticated methods, but most incidents are driven by straightforward techniques that exploit basic oversights.

Most cases involve:

- **Known vulnerabilities left unpatched.** Attackers continuously look for weaknesses.
- **Compromised credentials.** Password reuse, phishing, or weak authentication provides easy entry.
- **Improperly secured remote access.** Lack of MFA leaves doors wide open.

## EDGE DEVICES

Edge devices are a growing area of concern – systems that sit at the boundary between a corporate network and the wider internet (firewalls, VPNs, routers, etc.) Over the past 24 months, attackers have increasingly targeted these devices. Once compromised, they make entry into the network much easier.

This is compounded by the fact that edge devices are difficult to monitor and investigate, often not designed with security in mind. Even if patches are released, they don't automatically eject intruders who may already be embedded in the network. It was noted that the pace of this activity is outstripping the ability of many organisations to respond.

# THE FUNDAMENTALS STILL MATTER

**"THE INCIDENTS WE'VE OBSERVED HAVE SHOWN THAT ORGANISATIONS WHO HAD A PLAN RECOVERED SIGNIFICANTLY BETTER THAN THOSE WHO DIDN'T."**

It was discussed how preparation defines how an organisation weathers a breach. Despite the excitement around advanced detection technologies, the fundamentals remain key:

- **MFA across accounts and remote access.**
- **Strong account and access management to prevent privilege escalation.**
- **Strong network segmentation to contain attackers if they gain entry.**

These measures, though sometimes tedious, consistently reduce the likelihood and impact of incidents.

Other suggested priorities included:

- **Knowing your network.** This is especially critical during mergers and acquisitions, when legacy or unpatched systems may be inherited without full visibility.
- **Managing supply chain risk.** An organisation is only as secure as its weakest supplier. Overlooking third-party access or security practices leaves critical gaps.
- **Exercising your plans.** Too many incident response plans are written, filed away, and forgotten. It's imperative to rehearse and test them regularly. Are contacts up to date, do staff still know their roles, can external partners be reached quickly?

# ACTIONS IN THE FIRST FEW HOURS

Small organisations often ask all 3 of our representatives, **"Why us? We're too small to be a target."** Their answer was that, in fact, they're rarely targeted directly.

Most attacks are part of a volume game designed to exploit small mistakes at scale rather than singling out victims, in contrast to spear-phishing attacks which are targeted and specific. This underscores the importance of preparation.

All representatives suggested that immediate priorities should include:

### KNOW WHO TO CALL

Legal, PR, insurers, law enforcement, and technical responders must be contacted quickly. What's more, knowing how to contact them if your systems are down. Who does what, what are their contact details, what are your agreements?

### AVOID LAST MINUTE IMPROVISATION

Organisations without insurance often find themselves desperately searching online for an incident response provider in the middle of a crisis. This wastes precious time, significantly increasing costs.

### RECOGNISE THE BREADTH OF THE INCIDENT

Breaches impact the whole business. From data mining to regulatory liaison, recovery requires coordinated effort across functions.

### ENGAGE WITH THE NCSC AND NCA EARLY

It was noted that the NCA and NCSC are not regulators. They're available to provide support, but nothing is shared with regulators without consent. Engaging with them, however, can demonstrate good faith, showing that the organisation is willing to cooperate.

# CRISIS COMMUNICATIONS

Communication emerged as one of the most impactful aspects of response. All perspectives converged on the same message: **what you say, when you say it, and how you say it will shape how you recover**.

## DON'T RUSH

Early definitive statements are risky, as the full nature of the attack is rarely understood at the outset. Don't overstate the nature of an attack in your communications. Describing a basic incident as "highly sophisticated" will likely damage credibility later.

## AVOID RETRACTIONS

Correcting inaccurate statements damages credibility and distracts from remediation.

## PRE-PREPARE HOLDING LINES

Draft generic but adaptable statements in advance. During the panic of a live incident, starting from scratch is a recipe for mistakes. Involve communications experts – your marketing or PR team. These are things you can do today.

## COMMUNICATE SECURELY

If parts of your network are compromised, don't rely on internal systems to coordinate your response. Establish crisis communication channels in advance and use familiar systems. Test them regularly and ensure that has access and awareness.

## TAILOR MESSAGES

Different audiences (staff, suppliers, regulators, customers, the media) need different levels of detail and tone. Defining that level is something you can do today, rather than amidst the panic of an incident.

**"HOW YOU COMMUNICATE WILL DETERMINE HOW YOU RECOVER AND HOW YOU ARE REMEMBERED."**

# THE HUMAN SIDE OF CYBER SECURITY

Organisational culture often defines outcomes. The experts repeatedly stressed the importance of empathy and psychological safety. Cyber security professionals operate under immense pressure. Providing emotional support during and after incidents is vital.

A no-blame culture fosters resilience, as complex IT environments mean mistakes are inevitable. Therefore, blaming individuals is counterproductive; instead, focus on systemic improvement and shared responsibility.

Strong cultures also break down silos. IT and security teams must be empowered to communicate openly with the wider business. Giving technical staff opportunities to explain issues in plain language helps demystify risks and build organisational support.

**"YOU MUST AIM TO DO THE BEST YOU CAN WITH THE SITUATION YOU'VE GOT. PERFECTION DOESN'T EXIST."**

# LESSONS LEARNED

Across all three perspectives, several common lessons stood out.

## NATIONAL CYBER SECURITY CENTRE:

- Incidents are marathons, not sprints. The first 48 hours are only the beginning.
- Team wellbeing is critical. Arrange practical support such as rest, food, and accommodation. Burnout reduces effectiveness and prolongs recovery.
- Keep records. Assign someone outside the immediate technical response to take notes and log decisions. Good documentation saves time and aids post-incident investigations.

## NATIONAL CRIME AGENCY:

- Debrief every incident. Document what worked and what didn't.
- Test plans continuously. Response plans degrade over time. People leave the business and roles change. Regular testing keeps them effective.

## CYBER INSURANCE SECTOR:

- Backups are non-negotiable. Maintain clean, offline copies of critical data that cannot be encrypted by attackers.
- Practise good data hygiene. Reduce the amount of sensitive data you hold. If benign data is stolen, the impact is far smaller.

# CONCLUSION

Cyber breaches are unfortunately now inevitable. Organisations that focus on the fundamentals, plan and exercise their responses, communicate carefully, and support their people are consistently better placed to recover with their reputations intact. With preparation, clarity, and compassion, it's certainly possible for organisations to a cyber security breach.

# PRACTICAL CHECKLIST FOR ORGANISATIONS

- Patch and secure edge devices.
- Implement MFA across all access points.
- Maintain and regularly test incident response plans.
- Map supply chains and ensure supplier governance.
- Establish secure crisis communication channels.
- Keep offline, tested backups.
- Remove unnecessary or archived data.
- Draft and maintain external and internal holding statements.
- Provide wellbeing resources for response teams.

# RESOURCES

**National Cyber Security Centre (NCSC):**

- Cyber Essentials – guidance on defending against the most common cyber-attack vectors.
- Incident Management Guidance – steps for preparing and managing security incidents.
- Communications Guidance – advice on messaging before, during, and after a breach.
- Organisations Considering Payment in Ransomware Incidents – guidance on the risks, legal issues, and decision-making around ransomware payments.
- Find an Assured Cyber Resilience Audit (CRA) Provider – directory for accredited auditors who can assess your cyber resilience.

**National Crime Agency (NCA):**

- Cyber Crime – resources on threat types, reporting, and law enforcement collaboration.

**Reporting & Regulatory:**

- Action Fraud – the UK's national centre for reporting fraud and cybercrime.
- Information Commissioner's Office (ICO): Data Breach Guidance – the UK regulatory requirements and processes for personal data breaches.

**Best Practice & Frameworks:**

- NIST Cybersecurity Framework – a widely adopted framework for managing cyber risk.

# ABOUT CYRO CYBER

Cyro Cyber are your cyber security guardians.

We work with highly regulated, data-led organisations that know the stakes of getting security wrong; businesses that handle sensitive data every day, who need to know that their security measures are exceptional.

We offer a plethora of services, tailored to protect your organisation and meet your specific business needs.

**GRC**
Governance, Risk and Compliance

**CSA**
Cyber Security Architecture

**OST**
Offensive Security Testing

**CSS**
Cyber Security Services

# CYRO® CHAPTER

Rooted in a **people centric approach**, the Cyro Chapter is a **community** that offers **strategic insight, peer level collaboration**, and **fresh perspectives** to tackle complex, evolving threats.

- **COLLABORATION & CONNECTION**
- **KNOWLEDGE SHARING & INSIGHTS**
- **INNOVATION & LEADERSHIP**

**Register now to join an exclusive community and help shape the future of cyber.**

# CYRO® CYBER

YOUR CYBER SECURITY GUARDIANS


www.cyrocyber.com

hello@cyrocyber.com

Cyro Cyber