Breached? Meet the usual suspects…

Your guide to recognising how breaches happen and how to respond to them.

call **020 3855 5303** or email **help@normcyber.com**

norm.

Woop woop
it’s the cyber police…

At **norm. cyber** we know that when you’ve been breached the likelihood is that it is an internal affair. When that’s the case you need an impartial external team to investigate and get you back on track.

We’ve done some profiling on the usual suspects to help you be breach aware and know when you need a Cyber Security Incident Response Team (CSIRT for short)

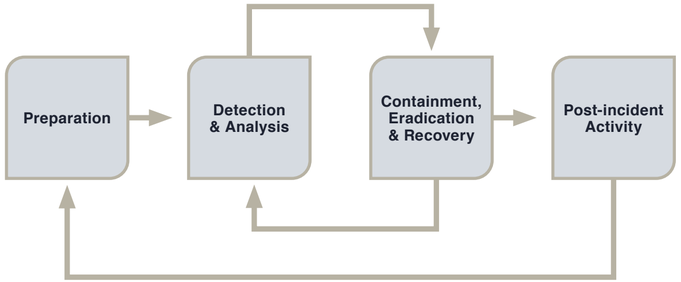
Names have been changed to protect the identity of the totally made up but quite relatable characters involved in the making of this brochure.

Been breached?

In the event of a cyber security and/or personal data breach, there are various well-established and proven best practices intended to minimise the impact of the breach and get back to “business as usual” as soon as possible.

Although it will vary according to the type and scale of the breach, and the nature of the affected organisation, typically the process follows the below stages, based on the NIST Incident Response Lifecycle.

* **Preparation**
* **Identification**
* **Containment**
* **Elimination**
* **Recovery**
* **Notification**
* **Review**



#01

Name: **Barry ‘Big Mouth’**

Profile: Barry likes to brag about sensitive information that puts his company at risk to show off. He doesn’t mean to cause harm but is not aware of the consequences of his loose lips.

Motive: Lack of discretion

How: Overheard by external cyber scoundrel

C.S.I.R.T
Cyber Security Incident Response Team

Usual Breach Suspect

You need a rescue plan

As with all incident response, preparation is vital. Primarily this equates to developing an incident response plan which identifies the key people, teams and procedures required to execute the plan and achieve the desired outcomes.

Traditionally, companies have developed their cyber security incident response plan and identified a team consisting of internal stakeholders and the owners of key decisions and actions. While this makes sense to an extent – who better to tackle an issue than the people who know the environment best? – there are also a number of significant advantages to involving an external specialist in breach management.

Here we assess the relative merits of each approach, and the difference they can make to minimising the financial and reputational damage caused by a breach.

In the case of a cyber security breach, the plan will also need to:

- ✔ Define what does, and does not, constitute a cyber security and/or personal data breach
- ✔ Determine a process for categorising the breach, which will depend upon factors such as whether personal data has been stolen, and if the affected organisation is still able to trade
- ✔ Detail the level of response required in each case according to the categorisation
- ✔ Specify how systems will be preserved for forensic examination
- ✔ Outline the procedure for deciding who needs to be notified and when – including employees, customers, partners, the ICO and law enforcement.

#02

Name: **Nora ‘The Internet Explorer’**

Profile: Nora is a freespirit who likes to explore the internet to no bounds. Unafraid in her endeavour she clicks quick, she goes where she wants and downloads freely.

Motive: Lack of awareness

How: Downloading unsafe applications

C.S.I.R.T
Cyber Security Incident Response Team

Usual Breach Suspect

Experienced Investigators

Almost without exception, the people who know the IT environment best are the people who design and manage it. Technology leaders and practitioners know the systems and applications in use, how they work together and their criticality to business operations.

The chances are that they will also be the first people to either discover or be informed of a security breach – either through anomalies in audit logs, alerts or malfunctions within the systems themselves, or reports from internal users and/or third parties.

What happens next largely depends upon this team’s previous experience of and exposure to security breaches and whether there is a proven response plan in place. The nature and severity of cyber security breaches varies wildly, and determining the extent of the breach is absolutely critical to its containment and remediation.

While most IT teams will have some degree of familiarity with security incidents, it may not be their primary focus...

External CSIRT providers live and breathe security incidents. They see it every day, across all industries and within all sizes of organisation. They are experts in getting to the bottom of what happened and how it happened, and have tried and tested containment and remediation methods.

The most comprehensive services also include provision for liaising with the ICO, if required, and guidance on communicating with customers and other stakeholders. How these engagements are managed will have a significant bearing on the financial and reputational ramifications of any breach.

#03

Name: **Billy ‘No Bonus’**

Profile: Billy believes he deserves more than what he gets. He’s missed out on a bonus and is out to make a fast buck and dish out some payback to his employers.

Motive: Disgruntled employee.

How: Selling confidential information to external sources.

C.S.I.R.T
Cyber Security Incident Response Team

Usual Breach Suspect

Chance isn’t such a fine thing

Not all cyber security breaches equate to a personal data breach, but the motivation behind many cyber-attacks is to acquire personal information such as credit card details, national insurance numbers and user credentials. There are far too many successful examples of this type of breach to name, but some of the most high profile include Marriott, Zynga and Equifax. While a fine from the ICO or other regulatory body is far from the only consequence of a personal data breach, it is the easiest to quantify.

Whichever way you look at it, both the number and severity of fines is increasing, with the average amount currently standing at **£250,000.**

For a list of recent enforcement actions taken by the ICO click here.

Determining whether the ICO needs to be informed of a security and/or personal data breach is the job of a data protection expert or DPO; preferably a qualified lawyer with experience of data privacy laws - such as the GDPR - and in dealing with the ICO.

Without exception, the ICO should be informed of a personal data breach as soon as possible. Even if the issue has yet to be remedied, the ICO tends to look more favourably upon organisations that demonstrate openness and clarity in the event of a breach. It will also assess the adequacy of the security measures that were in place prior to the breach, planned remediation measures and the controls that will be adopted to prevent a future occurrence.

If an organisation already employs a legally qualified DPO, it would fall within this person’s remit to liaise with the ICO and ensure that the company is represented in as positive a light as possible. The most comprehensive CSIRT providers will offer this as part of the service, and it can make a significant difference to the size of the fine issued – and indeed whether there is a fine at all.

In some instances, the ICO will be more lenient with upon organisations that appoint an external CSIRT provider, as it is viewed as an indication of its commitment to remedying the situation and minimising the impact on users.

*£250,000 is a big rainy day fund!

#04

Name: **Diedre “Distracted”**

Profile: Deidre works hard but can get easily distracted. She’s not unknown to leaving her laptop lying around and unlocked out in the open.

Motive: Lack of vigilance.

How: Sets passwords to “password”.

C.S.I.R.T
Cyber Security Incident Response Team

Usual Breach Suspect

The Blame Game

One of the major questions any organisation will ask in the event of a cyber security breach is “how did it happen”?

While the only party that is truly to blame is the perpetrator of the attack, the most likely scenario is that someone from within the organisation either missed something or made a mistake.

From unpatched servers to application vulnerabilities and users clicking on something they shouldn’t, the means with which attacks are executed are numerous.

One of the advantages of using a third party is that they will be completely independent in their analysis. Their motivation is purely to assess and remedy the current situation, and they have no vested interest in the effectiveness or otherwise of existing cyber security tools and processes. Their role is not to apportion blame, it is simply to ascertain the facts and help manage the situation accordingly.

In addition, using an external CSIRT service sends a strong signal to both internal and external parties. It indicates that an organisation takes its security and data protection responsibilities seriously, and recognises the importance of not only resuming normal levels of service but also protecting the privacy of its users and clients.

*We don’t look for scapegoats, whipping boys or people to blame but let the data to the talking

#05

Name: **Greg ‘The Unread’**

Profile: Greg is a dutiful, loyal employee. What he gives in enthusiasm, he lacks in phishing awareness. Unfortunately, he rarely thinks before he clicks.

Motive: Lack of training.

How: Phishing link.

C.S.I.R.T
Cyber Security Incident Response Team

Usual Breach Suspect

Who you gonna call?

An open line of communication from **norm.**

One of the disadvantages of using an external CSIRT provider can be the delay between incident discovery and commencement of the third-party investigation.

However, this need not be the case by engaging with a CSIRT specialist on a retained basis with agreed response times and SLAs.

Without this agreement in place, there is a risk of delay, as retained clients will take priority and remediation for on-demand clients may be on a “best efforts” basis.

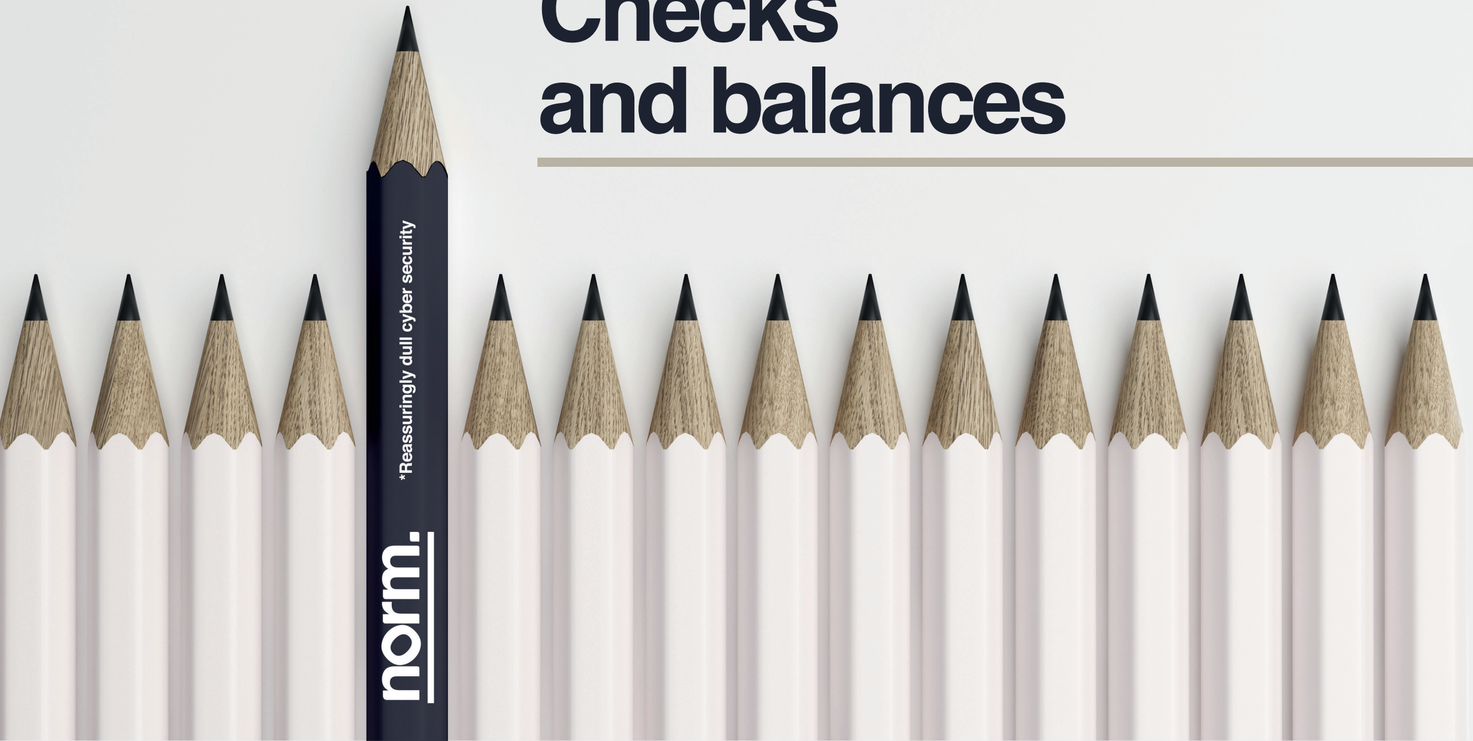
Some providers offer a middle ground, whereby companies can pre-register with them without signing up to a monthly retainer.

This initial engagement gives organisations the peace of mind of setting up the basics, without a budgetary commitment or an SLA in place.

Needless to say norm. provide all three services... just so you know.

Retained	**Pre Registered**	**On Demand**
Monthly retainer	Reduced day rate	Day rate only

*In case of emergency of any cyber kind you can always rely on the reassuringly dull cyber security that is **norm.**



Checks and balances

All bases = covered

There are pros and cons to using an external CSIRT service. Every organisation needs to decide which approach is best for them, and ask themselves the below questions:

* Do we have a cyber security incident response plan, and has it been tested?
* Are we confident that we have the necessary cyber security expertise in-house to respond to an incident quickly, and to minimise the damage?
* Do we have an in-house, legally trained expert in data privacy law, and do they have experience of liaising with the ICO?
* In the event of a cyber security breach, would we benefit from appointing an external party to validate our own response and plan of action?

Regardless of whether an organisation chooses to assemble an internal or external CSIRT, the principles and goals are the same, and preparing for a breach is crucial to the eventual outcome.

This means having a comprehensive response plan in place and the right people with the necessary expertise on the team, regardless of whether they are an employee or not.

We take cyber security seriously

*No really, all dogs aside - we are remarkably good at what we do.

To find out more about the **norm.** CSIRT service click here.
Or for the full **norm.** CSIRT data sheet click here.

If you require immediate assistance call us on
020 3855 5303 or email **help@normcyber.com**

To sign up to the norm. CSIRT pre-registration service,
email **CSIRT@normcyber.com**