cyberplus

POST BREACH

ARE YOU STILL VULNERABLE?

RESTORE YOUR CONFIDENCE

Cyberplus offer post breach services designed specifically to help recovery from a cyber-attack and restore full confidence to your company, brand and reputation..

RECOVERING FROM A CYBER-ATTACK

So you've suffered a cyber-attack, your systems and data has been compromised and your IT department has done all they possibly can to restore the systems to how they were before the attack. Nobody is going to be happy that they were the victim of a cyber-attack, but how do you feel about the way it was handled? Are you worried that there are still vulnerabilities that weren't identified? Do you have confidence that your organisation is now more prepared than before - could it withstand another cyber- attack?

RESTORE CONFIDENCE

Cyberplus provide organisations with a full Cyber Emergency Response service, making sure that your company is well prepared and ready to act in case of a cyber incident or an identified attack. This includes the preparation and planning that is critical in ensuring your organisation is ready and able to respond quickly and effectively from a minor incident or a major emergency.

"We were attacked and tried to fix things ourselves" How can Cyberplus help?"

Cyberplus can still help even when your IT team have already tried to fix the issue. The first thing Cyberplus do is make sure you are actually safe from further harm. Then we take a look at what happened using a combination of forensic analysis, scans and interviews with staff to help create a comprehensive report. Then it's a matter of demonstrating lessons learned and becoming safer and stronger after the breach.

For full details visit cyberplus.co.uk or email cir@cyberplus.co.uk

POST BREACH ASSURANCE SERVICES

FORENSIC ANALYSIS

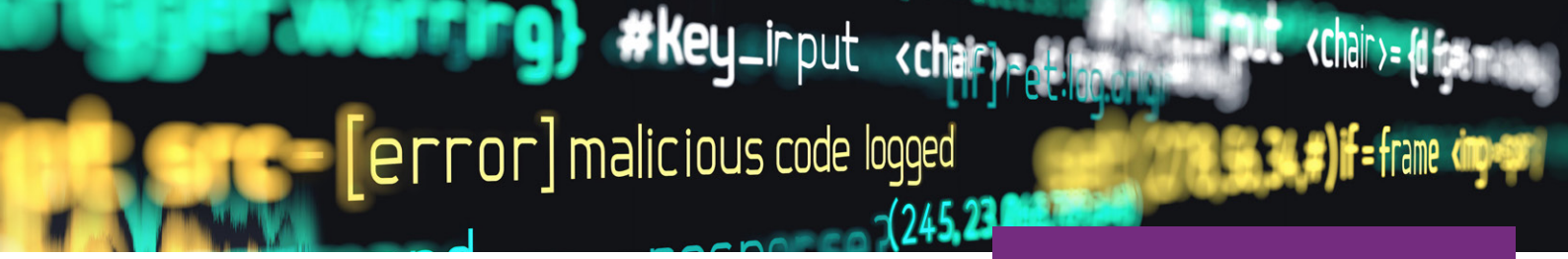
Our forensics team are trained to utilise advanced data recovery and forensic investigation techniques, preserving evidence and maintaining chain of custody, for presentation in court.

STATE-OF-SECURITY ASSESSMENT

We look for vulnerabilities in your organisation that could lead to cyber attacks, whether found on computer systems, processes or through people.

POST-MORTEM ANALYSIS

Through a series of interviews and analysis of the forensics we've managed to obtain, a report is created to summarise the cyber attack, including details and timeline of both the breach and response, concluding with clear lessons learned and demonstrable actions for improvement.



POST BREACH

WHAT'S ON YOUR MIND?

AM I STILL VULNERABLE?

Recognising there has been a cyber attack and identifying the cause is vital to containing the damage and eliminating the threat. Attacks are becoming more & more sophisticated and it's now common practice for attacks to act as a smokescreen for another. Not all attacks are announced and come with ransom notes. Attackers tend to try and stay hidden until they have explored for further security vulnerabilities they can find. Even if your team has recognised a specific type of attack, it is essential to investigate if the vulnerabilities that allowed them access are still there. Using backups to restore systems to a state prior to an attack may still leave an open door for the attackers.

WHAT WAS STOLEN/COMPROMISED?

Our investigation will try to identify areas of the organisation that were compromised including systems, data and user accounts. This is useful for communicating with both internal and external stakeholders, and can also be used to place a number on financial impact of the attack for insurance purposes.

HOW DID IT HAPPEN? WHO DID IT?

Perhaps the initial vulnerability was through weakness in your defence e.g. un-patched software, or through an attack on a third party supplier with weaker security defences, or through an act of social engineering on one of your employees or even be perpetrated by an employee? By identifying the cause, we can make sure that measures are put in place so it won't happen again.

CAN YOU HELP ME PROVIDE INFORMATION FOR REGULATORY OR INSURANCE PURPOSES?

Through a series of interviews and analysis of the forensics we've obtained, a full report is created to summarise the cyber-attack including details and timeline of both the breach and response. This report will help calculate the financial impact, which can be used for regulatory reports and insurance requirements.

HOW DO WE MAKE SURE WE'RE BETTER PREPARED FOR A CYBER-ATTACK?

Clear lessons have to be identified and learned and demonstrable actions for improvement must be actioned. Of particular importance is your organisation's strategy for cyber risk management. Is this mature and simply needs tweaking or is significantly lacking and needs better planning. Not all attacks can be prevented, and the increasing number of attacks mean that you're more likely to need to have a well prepared cyber incident response plan (CIRP) and a clear and a well-drilled incident response team (CIRT) who know their roles and can respond immediately when needed.

If you have already been the victim of cyber-attack, Cyberplus can help you get back up and running with confidence, ensuring you are more prepared to deal with future attacks.

For full details visit cyberplus.co.uk or email cir@cyberplus.co.uk

CYBER EMERGENCY RESPONSE

INVESTIGATION

The first step is always to gain an understanding of the current situation. This will include getting a timeline of key events, the data that has been collected, steps taken etc.

AGREEING OBJECTIVES

It is important to ensure that client objectives are practical and achievable. The goal is usually one - or a combination of the following:

- Identify data loss
- Recover from the event
- Determine attack vector
- Identify the attacker
- Confirm that there are no other undetected breaches

COLLECT EVIDENCE

Using advanced data recovery and forensic techniques, we ensure preservation of evidence to law enforcement standards.

ANALYSIS

The relevant analysis is carried out depending on the evidence collected and agreed objectives.

MANAGEMENT GUIDANCE

At all stages, management are guided by Cyberplus on the steps required to be taken including communications.

DEVELOP REMEDIATION PLAN & INVESTIGATION REPORT

Remediation will vary according to breach type and extent, as well as size and type of organisation.
The report will contain all parts of the response carried out as well as recommended actions aimed at preventing events and minimising the impact of any future attacks.

cyberplus

SPEAK WITH A TRUSTED ADVISOR TODAY:

+44 845 257 5903
cir@cyberplus.co.uk