# Ensure you are ready to Coordinate and Respond to your next Cyber Incident

Dealing with any incident is stressful enough, but when you lack the tools to coordinate and plan your response you will find your problems continuing to escalate until you can control and communicate securely.

CyberCPR was conceptualized by Logically Secure's active incident responders during their many years of work in the trenches of the cyber battleground. It is designed to be simple to use and to augment and support many aspects of incident management's key pinch points of visibility, accurate action and decision record keeping, secure communications and evidence management.



CyberCPR is featured in the SANS Institute's SEC504 -Incident Response and Hacker Techniques course (see www.sans.org), Demos are available. Contact us for details.

#### Extensive use of industry standard secure communications

prevents attackers who are on your network or in your midst from learning your remediation plans. We ensure this as CyberCPR provides simple-to-use in-incident chat, messaging and document sharing over encrypted (HTTPS) channels.



**Need to Know** Is enforced at multiple levels ensuring that those without a need to see an incident's details, evidence or analysis are prevented from even listing the case or searching for related evidence.

Workflows mean that regular tasks can be both delegated and monitored for completeness and progress. This allows newer team members to progress with less supervision, freeing up senior staff to focus on more challenging aspects of analysis and incident investigation.





### Separate Management Portal provides key leadership with real-time updates without burdening or deflecting analysts from their primary mission and tasking

Information flow is paramount in incident management. The CyberCPR Enterprise Management Portal (CPRMedic) provides an abstracted interface that gives oversight and statics at the touch of a button. Key details like incident updates and statistics over the last week, month and year are available immediately and securely over HTTPS, whilst implementing the need-to-know principle for CPRMedic access.



### Working an Incident now?

Logically Secure operates several CyberCPR instances from our Cheltenham datacenter. We can provide fast access to a secure instance of CyberCPR for either trial, demonstration or operational use. Contact us for details.



#### CyberCPR supports wider security regulations and requirements as it:

- Exactly identifies who accessed what investigation evidence in the portal.
- Grants, revokes or restricts access to an incident or case in seconds.
- Encrypts all evidence uploaded to the system.
- Provides chain of custody information.
- Records the IP addresses from where user's login and access case data.
- Constantly enforces the need-to-know principal.
- Can provide in portal analysis of memory images and logs uploaded as evidence.
- Providing an in-incident secure chat system that is fully logged and persistent.
- Flexibly developed to meet customer's needs and new requirements.
- Coded in the UK by UK security cleared developers.
- Available through UK HMG G-Cloud9.
- Patented in the United States.

# In-application analysis tools enable flexible

**USage.** Staff on mobile devices can still fully participate in the investigation as the analysis of large log files and even system memory image analysis leveraging industry leading tools like grep and Volatility<sup>™</sup> can be conducted over wireless and cellular networks provided the HTTPS interface CyberCPR is accessible from the device. This also enables in-the-field users to upload at the crime scene photos from their platform.



## Normandy Cheltenham, 305-209 High Street, Cheltenham, UK

www.cybercpr.com and www.logicallysecure.com Office: +44 (0) 1242 220040 (Mon-Fri 9am – 5pm)

#### A choice of deployment methods from onsite to on

a choice of **cloud** platforms including Rackspace, Amazon AWS, Microsoft's Azure or hosted by us in Cheltenham, you choose where your incident data resides.

Regardless of where it is hosted, we never see any of your data at any time. This ensures the incident management solution meets GDPR requirements from the onset.



CyberCPR<sup>™</sup> is Patented in the U.S. (details available upon request), all logos and screenshots are copyrighted by Logically Secure Ltd. Additional images on this sheet are licensed from shutterstock.com CyberCPR<sup>™</sup> is a Trademark of Logically Secure Ltd, a UK based company Number 05967368. All rights reserved. Volatility, Rackspace, Amazon AWS, Microsoft's Azure are all Trademarks of their respective owners they are external 3<sup>rd</sup> party products and services not owned by Logically Secure Ltd.