CYBERCRIME NEWS

ISSUE 20 • APRIL 2026

IF YOUR BUSINESS WAS HIT TOMORROW, COULD YOU RECOVER?

CYBER INCIDENTS LIKE RANSOMWARE CAN BRING ORGANISATIONS TO A STANDSTILL, ENCRYPTING ACCESS TO CRITICAL DATA AND SYSTEMS, DISRUPTING SERVICES, AND COSTING VALUABLE TIME AND MONEY.

The impact isn't just immediate either – Financial loss, legal implications, and reputational damage can affect long-term recovery and damage customer trust.

Taking simple steps now, such as ensuring reliable backups are in place, can make the difference between a temporary disruption and a major business crisis.

WHAT IS A BACKUP?

A backup is a copy of important data stored in a separate, safe location—such as the cloud or removable media—used to restore information if original data is lost, stolen, or corrupted by incidents like ransomware.

Think about how much you rely on your business-critical data, such as customer details, quotes, orders, and payment details. Now imagine how long you would be able to operate without them. This is the data you must ensure is backed up regularly and securely.

HOW TO CREATE BACKUPS - THE 3-2-1 RULE

IT IS VITAL TO KEEP MULTIPLE BACKUPS AND TO LOGICALLY SEPARATE THEM.

Maintaining resilient backups means that if one is compromised, at least one other remains. The most common method for creating resilient data backups is to follow the '3-2-1' rule:

- At least 3 copies of data
- On 2 different devices
- With 1 copy stored offsite 1 onsite

This strategy is popular because it scales effectively and can give you confidence that your critical data is safe from a localised incident.

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

DORSET POLICE

PRODUCED BY DORSET OPCC AND DORSET POLICE

STEPS TO CREATING A BACKUP

1. IDENTIFY WHAT DATA YOU NEED TO BACKUP

Your first step is to identify your essential data. That is, the information that your business couldn't function without. For example, documents, photos, emails, contacts, and calendars.

2. KEEP YOUR BACKUP SEPARATE FROM YOUR COMPUTER

Whether it's on a USB stick, on a separate drive, or a separate computer, access to data backups should be restricted so that they are not accessible by staff and are not permanently connected (either physically or over a local network) to the device holding the original copy.

Ransomware (and other malware) can often spread to attached storage automatically, which means any such backup could also be infected, leaving you with no backup to recover from.

3. CONSIDER THE CLOUD

Using cloud storage (where a service provider stores your data on their infrastructure) means your data is physically separate from your location. You'll also benefit from a high level of availability.

For information on how to decide what cloud provider is best for you, visit the NCSC: https://www.ncsc.gov.uk/collection/cloud

4. MAKE BACKING UP PART OF EVERYDAY BUSINESS

The majority of network or cloud storage solutions now allow you to make backups automatically. For instance, when new files of a certain type are saved to specified folders. Using automated backups not only saves time but also ensures that you have the latest version of your files should you need them.

5. TEST YOUR BACKUPS!

It is all very well having a secure backup, but have you tested it to make sure it works? It is crucial to regularly test your backups to make sure data can be restored quickly and successfully, for when your business needs it the most.

PROTECT YOUR BUSINESS

Backing up your data now is one of the simplest and most effective measures to protect your business from future disruption. By putting reliable backups in place your business can recover quickly, minimise impact, and continue operating.

DORSET POLICE

Dorset Police

Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

E cybercrimeprevention@dorset.pnn.police.uk
www.dorset.police.uk

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

Office of the Dorset Police & Crime Commissioner

Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

T 01202 229084
E pcc@dorset.pnn.police.uk
www.dorset.pcc.police.uk