Eastern Region Special Operations Unit

Regional Organised Crime Unit

COVID-19 CYBER & FRAUD PROTECT MESSAGES

Wednesday 13th May 2020

Today's topic is 'Business Continuity'.

Cyber-attacks are common and businesses that have not prepared for the worst will often not recover. Critical files encrypted by ransomware, hardware failures, premises flooded or phone lines down are typical threats.

A business continuity plan will keep critical functions running and address how to deal with customers, the press, suppliers and the workforce.

List all the activities that are mission critical. Prioritise the list and record how long you can afford to go without each. Is it minutes, hours, days or weeks? This is known as the 'Maximum Tolerable Downtime' (MTD).

1. What data or information is required? If there is a need to rebuild operations today in a completely different location with no access to any computers, what information is needed most? Think carefully about what data is mission critical.
2. Once the most important resources are known, spend time and money protecting them:
   - Are they password protected or encrypted, on a separate part of the network and are staff trained to handle and protect the information?
   - Is there replacement equipment, are data backup's up to date, stored offsite and regularly tested?
3. Share priorities with network support:
   - Is there a tried and tested checklist for recovery according to business priorities?
   - Will operations be restored before the Maximum Tolerable Downtime is reached? If not, alternative work-arounds must be considered beforehand.
4. Develop work arounds. This might include paper based systems, cross training staff or succession planning. It might include the hire of equipment, remote working or cloud computing.
5. Compile a list of third party contacts. This might include legal advice; law enforcement, utility companies, insurance brokers, technical support and PR.
   - Build a 'cascade list' using employee phone numbers to use in a crisis.
   - Plan who needs to meet, how often and how will they communicate if the primary site is out of action or phone lines are down? How will the media, customers and workers stay informed to stop speculation? Can pre-prepared statements be drafted? Can roles and responsibilities be allocated to save time later on?
6. **Test and refine:** Plans and checklists can be circulated to key personnel and feedback collected. One can also role play a disaster with critical team members and work arounds can be tried and tested.

Hot Topic

Smartphone contact-tracking system(s) work by logging each time two people are within a certain distance of each other for longer than a specified amount of time. When a user registers themselves as being infected, an alert is sent out to everyone they could have passed it on to.

The UK is trialling this in the Isle of Wight for a period and like the authorities in many other countries, NHSX has opted to use Bluetooth transmissions to keep track of each qualifying meeting. Alerts will then be sent anonymously, so users do not know who triggered them. This appears to have raised concerns about issues from privacy to battery life. We will be following this with interest but beware of the FAKE news and fake apps that may appear.

Help the NHS stop the spread of coronavirus in the UK
This app can let you know if you may have been near someone with coronavirus (COVID-19) symptoms.
Learn more abo

'Generous benefactor' scams leveraging COVID-19, where **a stranger asks you to pay an admin fee to help move a large amount of money from one country to another for a reward,** are also on the rise. These are similar to the 'Nigerian 419' scams (named after article 419 of the Nigerian criminal code) but the sender claims to be a rich businessman in Dubai.

Emails, advertising investments in Bitcoin, to "take advantage of the financial downturn" are on the rise. The emails contain a link to a website that explains how Bitcoin trading platforms work. This malicious link will steal credentials and/or get the recipient to download a virus.

Reporting

Reporting to Action Fraud can be done online or by calling 0300 123 2040.
To report offers of financial assistance from HMRC, contact phishing@hmrc.gov.uk.

This advice has been collated by the East Midlands Regional Organised Crime Unit (ROCU) and is intended for wider distribution to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the ERSOU Protect Team CyberProtect@ERSOU.pnn.police.uk or your local Force protect team.