East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

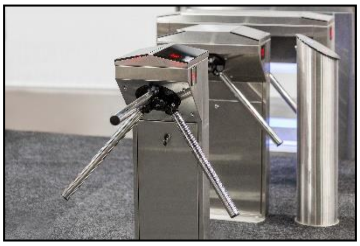
Thursday 03th September 2020

This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands Region 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 EMSOU Protect Team EMSOU Protect Team **or your local Force protect team.**

Today's topic is: Physical Security



Physical security is an important aspect of protecting any organisation. The aim is to control access and movement to protect employees, systems, critical processes and sensitive data.

This translates into controls such as; security fences, gates, turnstiles, mantraps, manned reception points, locked doors, locked filling cabinets, signage and placement of critical assets.

When choosing controls, look at a plan of the facility and consider the following:

- Which rooms are sensitive or critical to operations?
- What controls can be used to protect these locations?

The amount of controls and how much you are willing to spend on them depend entirely on how important the location is. For example:

- A room where employees are working on a new product design with high commercial value may require greater protection. This room might benefit from cipher locks, blinds, or should be centrally located within the complex.
- A loading bay or delivery point also constitutes a risk to most facilities because they frequently have unfamiliar people coming and going with easy access to the site. Increased monitoring and supervision of people in these areas is an absolute necessity. It is also important to consider how goods and deliveries will be secured and protected until they are internally distributed.

When protecting a site, most organisations will try to implement multiple check points to different zones to prevent unwarranted access to critical areas. Strong procedures are needed to add gravitas to these controls. For example, you might introduce rules about:

- The use of USB drives, and mobile phones in restricted zones.
- Out of hours working or lone working.
- The use of identity badges and challenging those without them.
- Visitor registration and monitoring.
- Leaving sensitive documentation on desks or internal telephone directories in plain sight.
- Use of privacy screens.
- Eating and drinking near equipment and leaving devices unattended.

Such rules and procedures need embedding as part of everyone's job description or formalised into mandatory policy so personnel know what is expected of them.

Like any other security threat, the risk of fire, flood, civil unrest or the dangers posed by contentious neighbouring organisations should also be translated into building design and staff training. These events tend to threaten continuity of operations. As do the loss of utility services, such as; electricity, water, heating, ventilation and broadband access. Organisations may:

- Regularly inspect and test these services as well as set up alarms to flag predicted outages.
- Develop a list of key contact points.
- Create multiple redundancies. For example, uninterruptible power supply (or UPS for short) enable IT system to perform a graceful shutdown whilst generators can usually keep systems active for hours, if not weeks.
- Finally, develop alternative methods of working. Many organisations are now weighing the benefits of cloud computing because they provide:
    - Metered usage - You only pay for services as and when they are required
    - Broad network access - Which permits stakeholders to work remotely
    - Rapid elasticity - Meeting IT infrastructure requirements quickly and easily

When discussing physical security, it would be remiss to exclude the effects of environmental conditions such as poor humidity, temperature and dust, which can dramatically influence the expected lifespan of equipment or the mean time to repair.

All businesses should conduct a risk assessment of critical equipment to ensure proper maintenance and operational procedures. This may include 'Heating Ventilation and Air Conditioning systems' (HVAC), warm or colds aisle, and cable trunking. Consider also the use of external specialist to carry out repairs and maintenance. Check that they are

- Suitably qualified and monitored when on site
- That confidential information is not exposed during maintenance, and
- Maintenance is logged so that the life expectancy and repair schedule is known.

This enables an enterprise to anticipate when a piece of equipment is going to cause a problem so that the people who depend on them are not adversely affected.

Lastly, many different security frameworks recognise the importance of monitoring equipment taken off site. If this situation describes your organisation then

- Formally authorise and log loaned equipment - perhaps based on a booking system that is periodically tested using spot checks or requesting that individuals demonstrate authorisation on demand. Not knowing who has what, is a serious data breach waiting to happen.
- Long term loans, however, should periodically require the employee to attest that the item is still in their possession, is in good condition and that they still need it to do their job.

Finally, all of these controls and procedures must be periodically reviewed and discussed to check adequacy and validity.

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.
Forward suspicious emails to report@phishing.gov.uk.
Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).