East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Monday 29 June 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: creating a cyber security-minded culture

In the aviation industry, where safety is the number one priority, the last thirty years have seen a radical cultural transformation. Unavoidable human error was rejected long ago, replacing this mind-set with a strong safety culture and a reliance on proven procedures. Little mistakes in aviation compound into huge problems.

This forced change, in the aviation industry, driven by the need for customer safety and confidence, is paralleled in the business world of online activity. Customer security and confidence is vital for businesses and organisations to survive and prosper.

In any organisation senior leaders must drive cyber security strategy, investment and culture to create operational resiliency. A culture of cyber security requires the senior leadership team (SLT) to:

- Invest in basic cyber security.
- Determine how dependant on IT business operations are.
- Approach cyber as a business risk.
- Lead development of cyber security policies.
- Build a network of trusted relationships to access timely threat information.

Staff are first line defenders and must become security aware and vigilant. To achieve a culture of cyber security:

- Leverage training resources through professional associations, academic institutions, the private sector and government sources to teach; security concepts, current threats and activities associated with best practices.
- Disseminate 'lessons learnt' and the benefits of reporting events to maintain ongoing vigilance.

Information is the life-blood of any organisation and critical assets and applications must be protected. Knowing where this information resides, and which systems and applications store and process it, is critical.

To achieve a culture of cyber security, organisations should have:

- Hardware and software inventories, to know what is in play and at risk.
- The implementation of secure configurations.
- The removal of unsupported or unauthorised systems.
- Automatic updates.
- Email and web browser security to protect against malicious emails and unsecured webpages.

Access to the digital environment must be tightly controlled in the same manner that physical surroundings are. To achieve a culture of cyber security organisations should have:

- Inventories of network connections (user accounts, vendors and business partners)
  - Multi-factor authentication for privileged accounts and remote access
  - Access and authorisation based on need-to-know and least privilege
  - Unique passwords on all accounts
  - IT policies and procedures for addressing changes in user status (transfers, termination etc.)

Even the best security measures can be circumvented. Organisations must learn to protect information where it is stored, processed, and transmitted and have contingency and recovery plans in place. To achieve a culture of cyber security, organisations should have:

- Lists of critical or sensitive information
- Knowledge of how data is safeguarded at rest and in transit.
- Automated backups and redundancies of key systems
- Protections for backups, including physical security, encryption and offline copies.

To respond and recover operations, it is important that an organisation reacts to a cyber-attack in the same way it might a fire drill or lockdown - with established procedures executed by knowledgeable staff. To achieve a culture of cyber security, organisations should have:

- The use of business impact assessment to prioritise resources and identify which systems must be recovered first.
- An internal reporting structure to detect, communicate and contain attacks
- In house containment strategies
- An incident response and disaster recovery plan, outlining roles and responsibilities.
- A list of who to contact for help, including outside partners, vendors, government offices, technical advisors and law enforcement.

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).