Thursday 06 August 2020

East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

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: Security Frameworks

Building a robust cyber security program is one of the ways to protect organisations from the constant threats presented in an online world. Employing a methodology to build and design a robust Cyber security program can greatly assist in this. A good framework aims to provide:

- **Long-term risk management;** offering an adaptive and responsive posture.
- **Bridge gaps;** aligning security with organisational goals.
- **Flexibility & adaptability;** providing widespread adoption and understanding.
- **Regulatory compliance**; planning for current and future needs.
- **Supply chain resilience;** often the weakest link and used as an entry point.

Frameworks allow an organisation to understand how good their security stance is and where it needs to be improved. It can be measured and classified using Tiers:

Tier 1 - Partial: There are no formalised security processes, reacting to risks and failing to share security information among its own workgroups. This may pose a security threat to partners and others.

Tier 2 - Risk Informed: There may be a security policy regarding risk management, but it is unlikely to be formally communicated to all levels, resulting in an inconsistent response to cyber threats.

Tier 3 – Repeatable: A formal policy is updated in response to changes in the business environment and threat landscape. Personnel are informed and empowered to respond to risks. There is clear communication between SLT, IT and the supply chain.

Tier 4 – Adaptive: Organisations actively managing their cyber security, learning from past incidents. Procedures to receive Intel from external sources, which is disseminated and acted upon. Risk management is built into the culture of the organisation with everyone able to identify and respond to new threats.

A way for organisations to self-assess is to apply the following list:

IDENTIFY:

- **Asset Management:** An inventory of all devices and software in the network and how information flows between them.
- **Business Environment:** Supply chain dependencies and resilience requirements for business continuity.
- **Governance:** Are formal policies and roles documented and communicated?
- **Risk Assessment:** Vulnerabilities identified, documented and prioritised
- **Risk Management:** Which risks must be mitigated and which can we ignore or transfer?
- **Supply Chain:** Do partners adhere to organisations cyber security standards?

Thursday 06 August 2020

East Midlands Special Operations Unit

PROTECT:

- **Access Control:** Are log-ins managed securely and is access based on least privilege?
- **Awareness Training:** Do users know their role in cybersecurity and trained to respond?
- **Data Security:** Is data safe when stored and in transit?
- **Processes & Procedures:** Changes to systems performed securely.
- **Maintenance:** Vulnerable systems maintained and documented to allow recovery.
- **Protective Technology:** Systems hardened from attack and audit log requirements determined, documented, and implemented?

DETECT:

- **Monitoring**: Establish baseline activity/process so abnormal network activity is apparent.
- **Detection**: Understand what suspicious activity looks like and identify emerging threats.

RESPOND:

- **Response Planning**: When to activate plans and how to elicit the correct response.
- **Communication**: Sharing information during and after an incident when needing to critically reflect.
- **Analysis**: Triage incidents, determining the most appropriate path forward.
- **Mitigation**: Isolating incidents to prevent spreading.
- **Improve**: Using post-mortems to improve planning and future actions.

RECOVER:

- **Recovery Planning**: A tested disaster recovery plan and a suitable backup strategy.
- **Communications**: Communicate internally and externally to restore reputation.

Creating a “heat map” of the results of the above analysis, will provide a strong visual guide.

	Current Tier	Target Tier	Risk Gap
Identify			
Business Environment	2	3	1
Asset Management	0	3	3
Governance	2	2	0
Risk Assessment	2	3	1
Risk Management Strategy	1	2	2
Protect			
Access Control	3	3	0
Awareness Training	2	3	1
Data Security	2	2	0
Process & Procedures	1	2	1
Maintenance	0	3	3
Protective Technologies	2	3	1

Prioritize: Determine your risk tolerance and which processes need the most protection.

Identify Current Tier: How well each of the categories is currently addressed.

Identify Target Tier: Determine the tier each control needs to be at.

Identify Risk Gap: Find the largest gaps between the current and desired tiers so appropriate resources can be allocated.

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).