East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Thursday 18 February 2021

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. 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: Supply chain security

Bringing goods or services to market often requires some level of dependency on other organisations. These may be suppliers, manufacturers, distributors, retailers or even service providers. Collectively, these 'supply chain' risks, must be carefully assessed and monitored, if the enterprise is to successfully mitigate cyber security issues.

An illustrative example:

In 2013, the US retail giant Target was attacked, supposedly by a Ukrainian hacker named Andrey Hodirevski or "Profile 958," as he was known to intelligence agencies. In all, the hacker stole 40 million credit and debit card numbers and 70 million records of personal information. How was such a feat accomplished? Through a simple phishing email sent to Fazio Mechanical Services Inc, Target's heating and ventilation suppliers.

The threat:

The problem, you see, is that cybercriminals often realise that a chain is only as strong as its weakest link. You may be armed to the teeth with cutting edge cyber security technologies, but if a trusted partner with access to your infrastructure isn't, you still have an exploitable Achilles heel.

What should I do?

Simple! You just need to ask a few pertinent questions before entering any agreement with a third party. If that ship has already sailed, then it is worth considering the following points retrospectively:

1. Does the organisation have a Business Continuity Plan (BCP):

This is important - a business continuity plan outlines how a company will continue to keep the show on the road without their IT up and running or in the face of some other form of catastrophe. Of course, having a plan and knowing if it works are two different things. For example, has the plan undergone any form of testing and how is it embedded into the DNA of the organisation.

2. Does the organisation have a Disaster Recovery Plan (DRP):
In the face of an IT meltdown, you need to know that your supply chain has already thought carefully about how to recover systems and services as quickly as possible. A good disaster recovery plan will identify the critical systems that support business functions and will detail the necessary workflows to enable their restoration.

3. Does the organisation use a cyber security risk framework?
Every business needs to consider risk. What threats are out there and what vulnerabilities do we have? What is the likelihood of these threats exploiting our weaknesses to wreak havoc? Not only will a risk framework identify these potential problems, but it will also help with the selection of security controls to mitigate these threats and pave the way to ongoing maintenance. The big players here are NIST RMF, Octave, ISO and ISACA.

4. Does the organisation use a cyber security framework?
Even if risks have not been considered lock, stock and barrel, an organisation may still use a security framework to help protect operations. A security framework will encourage the business to protect systems and processes from harm. For example:

- Physical security: To prevent unauthorised access to facilities or the delivery path of products.
- Employee training: To support the identification of security threats and elicit the appropriate response.
- User access and privileges: To enforce policies on who can access what, when, how, why and for how long.
- System hardening and patch management: To protect critical systems from unauthorised access or harmful malware.
- Network monitoring: To detect anomalous activity on the network and respond in a timely manner.
- Data protection: To protect the confidentiality or integrity of data when it is stored, used or when it travels from point A to B.
- Remote access: Aside from the obvious protection from man in the middle attacks, the longevity of access must be constantly reassessed.

There are many other issues a cyber security framework will address, but the take home message is whether your partners are demonstrating due care when it comes to looking after their own systems and yours. Look for ISO, NIST, Cyber Essentials – and for the cloud – standards akin to CSA CCM.

5. What does the Service Level Agreement (SLA) or contract say?
Despite every line of an SLA being an invitation to slumber, it is important to exercise due diligence by reading it.

The SLA will outline:

- The specific metrics associated with each service.
- What will happen if the metrics are not achieved?
- What caveats exist?
- What security standards will be maintained, along with your rights to audit compliance?
- Your rights to continue or terminate the service, as well as the associated costs of doing so.
- The roles and responsibilities of your organisation and the supplier.
- Disclosure of security vulnerabilities and incidents.

6. International considerations:

Since many of our readers are part and parcel of the UK Critical Infrastructure, we would be remiss not to point out risks when dealing with foreign organisations.

- Where do your suppliers operate and what ties do they have to their respective governments?
- How will local legislation, regulations and standards affect your dealings with your business partners, such as the protection and privacy of personal, financial, medical or proprietary data?
- Is there any evidence of corrupt or criminal activities? Supply chain compromises? Counterfeit products? What measures are in place to detect such things?
- Can the delivery path of products be guaranteed?

Tell me more:

Obviously the go to source for further information on Supply Chain Risks is the NCSC. But one might also consider ISO 2800 and NIST SP 800 – 161 for a more detailed and holistic approach to this super important topic.

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).