East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Monday 06 July 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 Cyber Insurance

In July 2019, more than 100 million customers had their personal information exposed following a massive data breach at Capital One, the fifth-largest credit card issuer in the US. Data breaches are not restricted to large financial institutions and we have seen them take place in; healthcare, airline, retail, restaurant, entertainment, social media, hotel, and manufacturing. Highlighting that any organisation can become a victim.

In addition to financial damage and reputational harm, data breaches have a significant impact on an organization's operational capabilities - Mondelez International, one of the world's largest snack companies, announced that "a global malware incident" affecting sales, distribution and financial networks cost them $54 million in 9 months.

The theft of stock from a warehouse would be covered by insurance, would the financial effects of a cyber incident be covered by your insurers?

General liability insurance does not typically cover cyber-related incidents. Legislative and regulatory changes regarding personal data, has also led to a sharp increase in litigation, instead, you will need:

First-party cyber insurance: which provides assistance to mitigate the financial impact of a cyber-incident to the business, such as crisis management and interruption costs.

Third-party cyber insurance: which picks up business costs for impacted customers; settlements, fines, attorneys' fees legal expenses etc.

Before purchasing a cyber insurance plan, organisations need to asses:

- What sensitive information do you hold and its value?
- The financial impacts of exposure - legal, regulatory or contractual penalties imposed?
- What systems are critical to performance and profitability?

The next step is to determine the amount of coverage, policies can mitigate the cost of:

- Diminished business operations and Incident response (e.g. forensic investigations).
- Notifying affected parties and offering Credit monitoring
- Crisis management & public relations
- Lost or stolen devices or data (hardware replacements)
- Legal advice & litigation brought by affected; employees, customers, 3rd parties and regulators.

Also note that the policy should go beyond traditional network security (e.g., denial of service or defacing of a website) to cover more recent attack vectors such as social engineering, phishing, or ransomware. The policy might also need to cover incidents that happen anywhere in the world and not just a specific country.

Managing the cost

When the retail giant, Target suffered a data breach in 2013, it failed to take account of fraudulent charges made on customers' payment cards, as well as the costs to replace such cards. Target also had to pay for expenses arising from the investigation and remediation of the data breach; credit-monitoring services, legal fees and advertising and consultancy fees to reduce reputational damage. The insurance policy ($90 million of cover) still left them with a staggering $162 million deficit.

Organisations exposed to risks that go beyond standard coverage, due to the nature of information collected or the industry in which the organization operates (financial services, healthcare, etc.) will require a bespoke policy.

Policy costs vary depending on the depth of coverage and analysis of assets and types of risks the organization faces.

When speaking to an insurance provider, ask questions to understand the types of incidents covered as well as the events or circumstances not covered.

To help we have created a Cyber Insurance checklist, email here, to receive a copy.

Review: Cybersecurity risks change all the time, and organizations need to reassess risk and risk appetite so that the correct coverage is maintained. Frequency of review depends on new work practices, equipment, or technologies that have been introduced. Typical insurance cover exclusions:

- **Thresholds:** Policies commonly set a limit on the coverage amount. Failure to assess the level of risk, may result in asking for too much or too little cover.
- **No Coverage for Non-Encrypted Information/Ransomware Payments:** Many cyber insurance policies specifically exclude confidential or personal information that has not been encrypted nor reimburse ransomware payments to criminals.
- **No Coverage for Fines** In many EU countries, insurers are forbidden from reimbursing a fine imposed by a regulator and the cost of enforcement actions.
- **No Coverage for Vicarious Liability**: Organisations relying on third party providers cannot delegate the liability for data breaches to the provider and the risk will still remain.

Hot Topic:

A new variation of a COVID-19-related HMRC phishing scam is targeting the passport, personal and banking details of the self-employed. A text is sent to the target pretending to be from HMRC, informing the recipient that they are due a tax refund. The recipient is sent to a fake, HMRC-branded site entitled "Coronavirus (COVID-19) guidance and support." Which is used to steal personal data.

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).