Intelligence Bulletin 12/02/19

Securitas Intelligence Unit

Managing Cyber Threats: Cybersecurity Tips for Businesses

The surge in online activity over the last few years has presented huge advantages to businesses. Despite the benefits, the new internet environment has also brought risks of cyber-attacks and attempts to steal information or money, causing operational disruption. Larger corporations typically have the capacity for organisational resilience in the event of a breach, whereas small and medium-sized businesses may struggle to respond and recover. It is vital to manage the risks of any cyber-threats and the current cybersecurity climate can seem overwhelming. An overview of current cyber trends can be found in the previous instalment in this cyber-focused series. Raised awareness of threats combined with the following steps can help bolster cybersecurity efforts:

Basic Online Security Tips

It is important to understand the nature of the data your business is collecting. Auditing and categorising data into low, medium and high risk identifies which data would prove the most harmful if leaked and can help determine the level of necessary protection. Any data that would greatly impact the business if lost or stolen should receive the highest security and have the most access control. Poor password hygiene is one of the simplest problems to rectify yet is the most common weaknesses exploited by hackers.[1] Hackers often sell exposed data, and if the same passwords are used on multiple systems, hackers can gain access to further sensitive information. Encouraging employees to use complex, varied password combinations and to use a password manager can help prevent further breaches. Multiple authentication methods are stronger than passwords alone. Using further authentication factors such a security questions or fingerprint recognition can help protect customers and employees from 'credential-stuffing' attacks.

Cybersecurity Awareness in the Workplace

Reinforcing a culture of cybersecurity and password training for employees is essential to avoid threats. Email continues to be a weak point in cybersecurity. Data loss and phishing attacks are the most prominent threats.[2] Phishing simulation tests can assess employee awareness and can evaluate training needs. An email security solution that encrypts messages and makes it easy to identify the origin of emails can make harder for employees to fall for phishing attempts.

Combatting Cybercrime

As discussed in the previous article, insider threats are increasingly concerning. Conducting an inside threat analysis assesses which current/former employees, contractors and third-party data suppliers have access to internal IT infrastructure and can help identify any vulnerabilities. Forming an effective contingency plan and an incident response team can help establish protocol in the event of an attack. Keeping employees aware of the response plan will help remind them of their responsibilities. Businesses may want to consider enlisting a designated PR liaison and developing a public response to communicate any threat, risk and harm to customers.

Building Cybersecurity Resilience

Employ what is known as a 'white hat' hacker. White hat hackers provide penetration testing and highlight any security vulnerabilities of an organisation's information systems.[3] Ensure all IT systems are only accessible through strong authentication or granting limited access to certain privileged users. Corporate IT networks should not be accessible from one central point. If networks are separated, hackers cannot control any further systems by gaining access to one network. Stay in control of the flow of data. Data is becoming more complex as our technologies improve. Keeping track of how data moves around your organisation, where it is stored and how it reaches its final destination can improve security. Security strategies should be consistently updated and revisited to respond to emerging threats.

[1] https://www.globalsign.com/en/blog/cybersecurity-tips-for-business/

[2] https://www.sungardas.com/en-GB/company/resources/articles/10-cyber-security-tips-for-any-growing-business/

[3] https://www.itpro.co.uk/hacking/30282/what-is-ethical-hacking-white-hat-hackers-explained

If you would like any further information on any of the elements mentioned in this bulletin, please email the Securitas Intelligence Unit at: