NABA Recommendations on Cybersecurity Training and Awareness

Draft # 3

Introduction

Employee training on how to detect and mitigate cybersecurity threats is critical to the on-going health of the enterprise.

Comprehensive security training and awareness should be undertaken in the enterprise on a reoccurring basis and should include such items like: social engineering testing; simulated phishing attacks; etc. Training should focus on implementing enterprise-wide behavioural change on the part of the employee and should be performed on an on-going, proactive basis.

Further, employees should be trained to adopt a "zero-trust" attitude toward external requests. In fact, employees can be encouraged to "think like a cyber criminal" to reinforce their preparedness.

Best Practices

Make the Enterprise Cybersecurity Policy Clear to All Employees

- Ensure the organization has a Board of Directors- and senior management- approved policy on cybersecurity, clearly outlining the strategy and tactics to achieve this policy and its implications on all employees. The resultant cybersecurity training efforts should be an executive priority that the Board of Directors, CEO, Vice-Presidents and other senior management staff all support.
- The Board and senior management should include cybersecurity threats to the corporate risk register. This will ensure the full implications of these threats are identified and mitigation plans are documented and tracked as they are put in place.
- Ensure employees understand that all corporate devices issued for their use remain the property of the company and as such, are governed by corporate policies and procedures. Such devices are not the property of the employee.

Adopt a "Zero Trust" Approach to Cybersecurity

- A "Zero Trust" approach to cybersecurity is predicated on the concept of "never trust, always verify".
- In this approach, all devices, email requests, etc. are to be considered suspect, irrespective of ownership, authorship, location or the fact they could have been verified previously. Therefore,
    - Train employees to adopt a "zero-trust" attitude toward all external and internal requests.
    - Create a vulnerability management program to eliminate technical debt from the organization as unsupported systems are a primary vector for malicious actors.
    - Gain insight into emerging threats by subscribing to and reading CVE (Common Vulnerabilities and Exposures) bulletins and taking appropriate actions.

Encourage Employees to Take Responsible Care of their Devices

- Ensure that the organization has and maintains a 100% accurate inventory of all devices that are allowed to access any internal network. If there are devices accessing internal networks that are not identified as corporate devices, immediately confiscate them and/or deny them continued access to any network resources.
- Ensure that all security patches are applied as soon as required and are not delayed by employee tardiness.
- Ensure that any employee device that has either been retired or replaced by a newer model is returned to the enterprise IT or cybersecurity department.
- Ensure that all devices of any employee who has left the enterprise be retuned to the enterprise IT or cybersecurity department.
- Ensure that all mobile devices have appropriate segmentation between corporate and private applications, if the latter is permitted.
- Ensure employees understand how to create complex passwords and change them at regular intervals.
- Ensure multi-factor authorization is enabled on as many applications as possible.

Teach Employees How to Spot Suspicious Activity

- Employees should be trained to identify some of the tell-tale signs of suspicious activity on their devices, such as: new text messages with imbedded hyperlinks; device sluggishness; additional start-up or boot steps; slow keyboard reaction times; etc.

Collectively Examine Individual Cases of Cybersecurity Breaches

- On an ongoing basis, review prior cases of cybersecurity threat or breaches with employees to educate them on how such threats can be successful in their own enterprise.

Run Simulated Cyber Attacks, Gather Metrics and Retrain

- On a regular basis several times a year, run simulated phishing and social engineering attacks across the entirety of the enterprise, including the C-suite.
- Gather metrics on those employees who fail these trials and offer specific training.

Track Training Compliance

- As a minimum guideline, cybersecurity training of all employees should occur once a year.
- Consultants/contractors working in the enterprise and accessing internal networks should be given the same training as employees. If they are excluded, it should be verified that they have been adequately training by their own company.
- Cybersecurity training of each employee should be monitored and tracked by HR or by some other internal party so that all employees receive the necessary training.

Continuously Monitor Threats

- Companies should consider joining/monitoring platforms that share anonymous information in real time about cybersecurity breaches, like the Media and Entertainment Information Sharing and Analysis Center (ME-ISAC) or other systems.

Make Cybersecurity an Ongoing Conversation

- Ensure employees understand that their role is fundamental to the success of any cybersecurity programme.
- Engage employees through regular workshops, seminars, etc. on their perceptions of the enterprise cybersecurity programme, including areas for improvement.

Draft #3

October 25, 2022