Employee Cyber Hygiene Training Options

Prepared by the Bloustein Local Government Research Center

Members can meet the Cyber Risk Management Program requirement for employee cyber hygiene training (Tier 1 - at least one hour spread over two years) in several different ways. When considering their approach, JIFs and their members should consider: 1) the technology and cybersecurity risks they face, as measured against 2) the quality and elements of the training program and 3) the cost. As in most risk management training programs, there is a direct correlation between the three elements. The better educational quality programs address a wider range of risks and are of better educational quality but cost more. The following graphic adds depth to the issues to consider; an explanation of the different types of programs follows:

Training Quality	•Different video styles may appeal to different audiences •Phishing tests increase the value and reduce risks •Level of customziation desired
Phishing Tests	•Cost is either fees to vendor or time spent by local program manager to customize testing
Program Overhead	•Staff needs to be assigned to manage the program, track employees, and decide what training is used.
Accountability and Cost	•The most flexible programs are the most accountable and have higher costs (fees plus time of local manager); The least flexible and accountable are the least expensive
Pricing	•Prices vary by: •Level of service provided by the vendor (higher price) as opposed to effort provided by customer (lower price) •Customization of training material
Flexibility	•Different vendors have different approaches and options •Some provice collateral printed and onlne material, periodically refreshed

Review and Analysis of Cyber Hygiene Services (*Fall 2017)*

Overview

All of the reviewed providers[1] offer online cyber hygiene (a.k.a. security awareness) videos and phishing training (companies only doing phishing training were excluded), and all do the same things with similar user enrollment and management reporting tools. The depth, pricing, management feature flexibility, and to some degree, the quality/style of videos are what differentiates them, making choices very JIF/member-dependent. While pricing is driven by the number of participants covered by contract, general pricing runs in the $8-$15/employee/year range (often based on a training service fee plus a phishing service fee), with variations driven by phishing training management, customization needs, and personnel (i.e., who manages the administrative overhead).

Generally, company-managed overhead will be slightly more expensive than a management by a local official or JIF. Depending on the service, member maintenance may require the time and attention of a JIF or member staff person to manage that aspect. Deciding on a vendor may hinge on the capacity of the JIF or individual member to handle the effort required by its choice of service.

All vendors tend to update their material regularly as cyber threats continuously evolve. There are various industry perspectives on how to deal with some cyber threats; different vendors offer different guidance on how to do so; there might be minor differences on how those recommendations affect local governments, but these are not substantial issues. It is important to note most of the videos are focused on private businesses, and the nomenclature reflects that; however, the risks and solutions are generally the same. One vendor (PivotPoint) has developed videos specifically for MEL municipalities.

The videos all differ by style (lifelike animation, cartoon, or live actors) and approach (from serious to relaxed), though the content is similar. All include interactive quizzes to reinforce the videos. National vendors also provide various types of free collateral materials designed to reinforce training. Phishing services involve sending emails to employees to see if they can be fooled into clicking on a dangerous link. Each vendor has a different approach and will propose various options to dealing with this form of penetration testing.

---

[1] *Research began using the Gartner Group's "Magic Quadrant for Security Awareness Computer-Based Training" 10/16 (most recent available when researched). Six of the vendors were selected from "Leader's" quadrant (high ability to execute and completeness of vision), then reduced to those who services seem most relevant to JIF need (i.e., US –focused, end-user security training, and phishing testing, plus two NJ based firms that JIF member have worked with.*

Phishing Test (Online) Service		
Service Level	**Sophistication of Test**	**Costs**
Best	*Fully customized templates and schedule*	*Fees and management time and attention vary by service provider*
Better	*Limited templates and schedule*	*Limited management engagement*
Marginal	*None*	*None*

The following analysis is organized into two vendor categories: New Jersey-based companies and large national ones. Following the analysis is a review of criteria that can be part of a contracting decisions (Training Management Considerations).

NJ-Based Vendors

D2Cybersecurity/Kean University

www.d2cybersecurity.com/industries/municipalities.html

D2 specializes in developing cybersecurity education and training for all levels of government and various private sector industries. It has a full line of videos that, depending on the level of service desired, can be branded or customized with the appearance of organization officials (this option requires video recording). Its program is made up of 8 individual modules. Terminology tends to lean corporate, but not overwhelmingly so. Each module has an interactive quiz. It has a contract and marketing arrangement with Kean University that effectively eliminates public contracting issues (over $17,500 or $40,000 if that becomes an issue). D2's phishing service has 25+ sample templates it can modify based on specific needs or target groups (i.e., police may get something targeted to them). The company manages the overhead; the user works with them to determine what they want. Extreme customization for a specific user group might result in additional costs, but it appears flexible. Members only need to provide email addresses of employees, but deeper customization is available (depending on complexity, there could be a fee). If contracted by a JIF, it will provide an aggregate, anonymized management report to the JIF, and a detailed report to the member. D2 has a representative (Brian Lau) available to meet with members considering its services.

PivotPoint

www.pivotpointsecurity.com/security-awareness-training/

PivotPoint has developed a video training series specifically targeted to NJ municipalities[2]. It uses a personally narrated, less formal, self-deprecating, tongue-in-cheek humorous approach; this is different from the other firms (the video presenter is John Verry, the head of the firm). It was developed by technologists (other firms

[2] *This was informed in part through a contract PivotPoint has with A.J Gallagher managed JIFs; partly developed on the possibility of obtaining work with other JIFs*

combine education specialists and technologists) and includes some superfluous technology jargon and detailed administrative information that are not present (and sometimes not relevant) in other vendor videos. The videos and site features are not fully active, but it is anticipated this will be addressed over time[3]. Given its interest in specifically serving JIFs, it has the capacity to meet with JIF officials to customize content. It uses a third-party service to manager its phishing program. As such, it has limited mailing flexibility, customization options and a smaller number of templates and landing pages. These limitations are offset by reduced management overhead. Mailings go to enrolled users; the service sends a link to management, who resends it to employee-users so they can self-enroll. A management dashboard provides basic reporting functions for video use and phishing.

Large National Vendors

The following vendors (in alphabetical order) are very similar in capabilities and approaches. All services are highly automated with dashboards and pick-lists to manage the process. They compete with each other and, over time, generally match each other's features. Video styles are varied. The narratives below are a summary of highlights from observations, limited demonstrations, and, in some cases, discussions with representatives. The firms all have website links to contact representatives who can discuss details for specific potential clients (the study made specific contacts with staff from MediaPro and Wombat, and information about KnowBe4 was obtained from its website and some JIF users of the service). The Gartner Group maintains a user review site of "security awareness computer-based training" companies. The three companies are all included (among others). This can be seen here: www.gartner.com/reviews/market/security-awareness-computer-based-training

KnowBe4

www.knowbe4.com/

KnowBe4 is a full-service application including assessment tools, phishing/attack simulations, education modules, collateral materials, ongoing training and phishing ID software tools. It has multiple short modules and longer comprehensive ones from which the member can choose. It also provides a Microsoft Outlook "add-in" feature that lets a user report a phishing attack to it (available separately for a small fee, but installation requires technical skill). System management is highly automated, providing the member a high degree of customization, though it requires the thoughtful attention of a local coordinator to take advantage of all the features (including developing individualized, or edited templates, customized unlimited phishing emails and penetration attempts). Due to its high level of automation and member responsibility for making it all work via dashboards and menu-driven options, its per user cost tends to be lower than other services. KnowBe4's services, support,

[3] *These issues have been brought to their attention and will likely be addressed in future revisions.*

sales and technical support staff are available through its website. It also provides a free phishing test (up to 100 employees).

MediaPro

www.mediapro.com

Media Pro is a full-service application including assessment tools, phishing/attack simulations, education modules, collateral materials, and ongoing training. It provides a very flexible platform with a wide variety of training packages that permit a "build your own" approach of mixing and matching interactive animated and photo-realistic videos from a wide selection of topics. Its videos include interactive quizzes and tests. Its integrated phishing dashboard has templates, but permits users to edit them and/or provide their own email. It also provides a variety of editable landing pages (the page that comes up when a phish is clicked on) with reinforcing videos that can be modified for specific users. Additionally, it has pre-packaged bundles that simplify the process. It would permit a JIF-based individual to manage the process for all member employees or permit a member who has a coordinator to handle training for the member. From a business standpoint, its representatives appear to understand government procurement issues and will work with resellers to handle RFPs. Its platform appears easy to use and allows a great degree of customization. Pricing is variable, based on the number of users and the services selected. It also has supplemental collateral materials, some of which can be locally branded.

Wombat

www.wombatsecurity.com

Wombat security is a full-service application including assessment tools, phishing/attack simulations, education modules, collateral materials, ongoing training and phishing ID software tools. Its videos run in 5-15 minutes modules, are interactive, and animated. It has various bundled packages, as well as the ability to customize packages. It has a phishing tool platform designed to send out emails. Pricing is variable; it can be purchased by the package or priced for individual modules; the more modules, the better the pricing. It also has an Outlook add-in if its phishing tools are used. It provides unlimited access to exercises. Its educational focus is on behavioral modification. Its pricing is a little different from the other companies; it charges extra if you want it to manage the process for you. It also provides a dedicated "customer success manager" who helps customize its platform and branding as part of its base service.

Training Management Considerations

Cyber hygiene training requires management time and attention in ways similar to, but may exceed, other employee training programs. Members need to address the typical aspects of training management, such as assigning activities to individual employees and tracking their compliance and progress. Furthermore, each form of cyber hygiene training requires different levels of management attention. For example, online services require enrollment of employees, usually done by providing the company a list of employee email addresses or providing employees a link for logging into the service. Most services provide a management dashboard that tracks participants' status and the results of testing.

If a JIF is going to administer the program, each member will need to assign an individual to work with a JIF program coordinator to ensure employee lists and participation are effectively managed. If members are going to administer their own program, the office or individual that usually coordinates employee training (often found in the human resources/personnel function) will need to add cyber hygiene to their portfolio. Whether tracking employee participation is managed centrally or in each department, internal management procedures must be established to ensure adequate recordkeeping and oversight.

The member's technology coordinator (by whatever title or function) should be engaged in decision-making for cyber hygiene training to ensure the risks presented to the member's employees are adequately addressed in the training program. Options include: selecting videos by subject matter or customizing the content of phishing emails. While the technology coordinator may not be an expert in employee training techniques, they have expertise in understanding the cyber threats presented to the organization. The coordinator should also be involved in reviewing the results of employee testing.

Finally, as in all risk threats, members should establish an incident review practice whenever a cyber incident takes place. Reviewing cyber incidents from a risk management perspective will highlight gaps in training or internal procedures that can lead management to make improvements in its activities and improve employee training. As in other areas of administration, if an employee is involved in multiple incidents, found to knowingly disregard training or other technology policies, or repeatedly fail the training, the member should employ progressive disciplinary actions in accordance with its disciplinary procedures in other areas.