Implementing an Effective Information Security Awareness Program

Presented by John Laffey

PJR Technical Manager

Before We Begin:

- All participants have been muted for call clarity
- The slides from this presentation will be available shortly from www.PJR.com – under “Training,” click “Past Webinar Slides”
- A recording of this webinar (and all past webinars) will be available for review on YouTube
  - Search “Perry Johnson Registrars” to view them – free!

PERRY JOHNSON REGISTRARS, INC.

Topics to be covered -

- Why an information security awareness program is critical to the success of your ISMS.
- What does your awareness program need to cover. What should it cover.
- Who and what to consider when creating your awareness program.
- Methods and frequency of delivering your training.
- How to measure the effectiveness of your awareness program
- Responses to questions asked during presentation

PERRY JOHNSON REGISTRARS, INC.

Information Security Awareness – Why is it Important?

- In my experience, people are the most important part of information security.
- With the rapid pace that technology changes and updates to software are made, the potential threat vectors and exploits related to them change just as quickly.
- One constant method of attack has remained, and that is to leverage the people who use and handle your information and systems in order to gain access to it.
- In many cases a data breach is the result of someone simply not knowing that what they were doing was unsafe, or could result in a breach.
- Having a well trained workforce can be the difference in suffering a data breach or maintaining the security of your data.

PERRY JOHNSON REGISTRARS, INC.

What Does Your Awareness Program Need to Cover?

- At a minimum your awareness program should cover the following:
- Where your organizations information security policies and procedures can be located and referenced by your employees so that they can be utilized.
- Who they should contact if they have questions about the policies and procedures.
- Who they should contact or what process they should follow if they have suspicions or concerns surrounding an information security incident.
- What the expectations are for your staff in terms of information security, and what the objectives of the information security management system are.

PERRY JOHNSON REGISTRARS, INC.

What Should Your Awareness Program Cover?

- In addition to the items in the previous slide, the following are a good idea to include in your training:
- Examples of information security threats specific to your organization, such as phishing e-mails, social engineering methods, and what your employees should do if faced with them.
- Explaining why information security is important using specific examples that relate to your organization. I have found that if people understand why something is important they are much more likely to follow the procedures to safeguard it.

PERRY JOHNSON REGISTRARS, INC.

Who and What to Consider when Creating your Awareness Program

- The audience – depending on the size of your organization it may be best to have a common set of awareness training material as all users perform similar functions with the same types of information security risks. For larger organizations with multiple specialized departments it would be more effective to have training material that is specific to the activities and information that they work with on a day to day basis. People tend to quickly lose interest if there are large portions of training that do not apply to them or their job role.
- The systems you use and the data you handle – If there are specific risks related to the information systems you use there should be training that is aimed at what your users need to be aware of. If there are specific handling requirements for certain types of data your organization processes, such as those outlined by HIPAA for health information, make sure that your staff know what they are or where they can find them.
- Administrative controls – For any information security controls that are administrative in nature, meaning that they are implemented in writing and are completely dependent on your staff following the direction of your policies/procedures, highlight what the expectations and requirements are for your staff and why it is important to do so. Again ensure that staff know where they can find the procedures/instructions that direct them so that they can utilize them.

PERRY JOHNSON REGISTRARS, INC.

Methods and Frequency of Delivering your Training

- While I favor instructor led training as it is typically more engaging, I acknowledge that computer based training (CBT) can also be effective. In either case it is critical that there are methods of evaluating the trainings effectiveness in place so that changes can be made if needed.
- At a minimum, information security awareness training should be part of the initial on-boarding process. Ideally it should be required to be completed prior to giving the new employee access to your systems.
- Requiring refresher training at regular intervals is also strongly advised, as threats and attacks tend to change at a frequent pace. In lieu of regular annual or bi-annual training, training must be given when there are substantial changes to your information systems or your policies and procedures.
- Awareness training should also include some type of quiz or test to ensure that the content is being understood. Additionally reinforcing new material with a test will give those administering the training some level of confidence that it is being understood.

PERRY JOHNSON REGISTRARS, INC.

Measuring the Effectiveness of your Awareness Program

- As mentioned previously, having a test or multiple tests/quizzes as part of your training course can give you a minimal level of assurance that the material is being understood. Additionally it can be useful to include a sign off for participants stating they understand and will abide by the information policies and procedures as part of the training to highlight the importance of it.
- Sending out a fake phishing e-mail to your users and tracking who clicks the (benign) malicious link is a great gauge of how effective your training was in terms of suspicious e-mails. There are some popular email providers that are beginning to include tools like this to administrators, as well as third party providers.
- Performing unannounced audits to see if users are abiding by clear desk and screen policies. Checking to see if users are writing down passwords on sticky notes and leaving them on their desks.
- Reviewing information security events or incidents, and determining if there is a gap in the material being covered or a lack of retention by the students. Internal auditing should also include questions to individuals regarding topics covered during the training to further evaluate its effectiveness.

PERRY JOHNSON REGISTRARS, INC.

Thank You for Attending!

Download these slides & view a recording at www.PJR.com.
Feel free to contact John Laffey with questions at jlaffey@pjr.com.

PERRY JOHNSON REGISTRARS, INC.

Questions & Answers

- Contact us for further information at 800-800-7910