Association of Institutional INVESTORS™

Topic A – Phishing testing and training

Repeating phishing exercises is important for raising awareness.

All users or a sample? In larger organizations if the objective is purely to measure the level of awareness, it's possible to start phishing with a representative sample. Sampling methodology is critical to align with your most critical risks (i.e. Executives, Sales, Privileged Users, client facing personnel, most critical IP owners, administrative assistant, HelpDesk employees, etc.). But it may be important to reach everyone if you are going to raise awareness.

How frequently? This depends highly on the awareness level of the organization, but in general we recommend to send out at least 4 emails a year in order to substantially increase the results. Contextualize emails as much as possible with known changes or event individuals can relate to in order to improve detection skills.

How to approach repeat offenders? It might be beneficial to focus on that group specifically. The range of action need to be in line with the risk profile of the individual. Low risk can be a notification to the person's manager and having to take an incremental on-line security awareness. Higher risk cases inclusive of repeated failure might lead to temporary suspension of privileged access previously granted, written documentation added to individual HR files and taken into consideration to annual review which might impact bonus / raises / promotion potentials.

A more positive approach to limit the user fatigue risk?

- Reward program for employee who identify and report potential issues
- Make training personal
- Reward positive behavior
- Consider targeted training for types of employees (not as practical at smaller organizations)
- Should be on-going and random
- Highlight the positives, not only the negatives of results
- Focus on the learning if someone falls for the test attack
- Make training fun, keep it short
- Offer prizes to those that show consistent positive results at the end of the year, show top departments maybe
- Alternate solution providers
- Provide your employees with a mean by which they can report phishing, provide phishing ideas or become phishing ambassador for large turn over groups such as call centers where you might want to visible representative / go to person for high level questions.
- Understanding your audience. For instance for Millennials customize phishing email to focus on company social events to help new generation become also aware of attack vector they might be less cautious about.

Topic B - Generational differences across firms

Corporate culture
Millennials value work-life balance and social consciousness. They value autonomy.
Enable staff to feel more impactful and see how they're contributing to the company's mission.
Emphasis on work-life balance (flexible work hours, working remotely from home,…) and social consciousness.

Empowering
Millennials want to own a project, run with it, and make a real, measurable difference.

- Allow people with less experience to access senior roles more rapidly.
- Including employees into the decision-making will help them think through their own contributions and projects in light of the company's bigger picture.

Desiring Feedback (Early and Often)
Millennials like to work independently.

- Give feedback along the way for employee motivation, so that they can integrate feedback into the final product.
- Balance of managing collaboratively and granting autonomy

Approach to Data Security
Millennials have never really known a world without technology and data, they grew up digitally engaged and they might see data breaches and misuse as unfortunate, but normal.
They've grown up with the personalization of content, and may be willing to give up significant portion of personal information, mainly depending on what they get back.

- Increase awareness and training around inherent risks
- Emphasis as very important that personally identifiable, financial, and medical data be shared only with those whom they have authorized access
- Reinforce importance of strong access security management. It seems that a significant portion of Millennials are less likely to use a digital resource or device if it requires complex passwords to use it, with a minority of them saying that they would like to see more secure and convenient digital verification and authentication methods available.
- Technical skills – more collaborative and technology-centric tools vs self-learning and instructor-led training
- Adapting to change – change is a norm in the workplace vs cynical about change
- Communication – collaborative, in person, and coaching style vs reserved and top-down authoritative coaching style

Topic C - Collaboration and general areas that asset manager firms should be focusing on

- New SEC released observations from its second round of cybersecurity examinations on August 7, 2017
- Benchmark data sharing (i.e. risk assessment rating)
- Market trend and impact analysis on sector
- Dash boarding / reporting to boards
- Board training and employee Security Awareness / Social Engineering training
- Sharing of information (success stories that benefit others), including Law Enforcement
- The above can be technical or otherwise
- Securing the endpoints (desktops/laptops/phones/tablets)
- IAM journey
- Cyber security cloud enablement / co-sourcing

Association of Institutional INVESTORS™

Topic D - Metrics around cyber and outside guidance on how to report

Top down/bottom up

- Identify nature of information expected by Board members / define risk appetite of boards
- Inventory of available information, and identification of additional feeds if necessary
- KRI construction
  - Threats
  - Incidents by severity, nature, impact, status opened/closed, root cause, …
  - Serious incident focus on corrective action plan
  - Testing and testing results (internal, third party internal control reviews…)
  - Employee training, results/trends of phishing exercises

- Qualitative
  - Key changes in the organization
  - Significant changes/new security related policies and procedures.
  - Regulatory

- CIS (Center for Internet Security) has created a metrics framework that members of CIS should consider.
- Create metrics that relate to your adopted control framework, for example NIST CSF (or use coverage areas)
- Metrics should be easy to capture (can always refine and start capturing other data points if needs aren't being met)
  - Good metrics
  - Enable decision-makers to take action
  - Are definable
  - Have context
  - Based on facts
  - Repeatable
  - Flexible
  - Granular and discrete
  - Relevant and Prioritized
  - Lean but comprehensive

- Cybersecurity Program score (maybe consider the maturity of the program and adoption of a framework to show where you stand)
- Incident summary of highs, medium and lows, show effectiveness of installed solutions
- Any outstanding issues not remediated since last security audit
- New security implementations since last meeting that have impact
- Indicate areas of concern (risk) and approach to minimize or mitigate
- Highlight known and unknown areas of cyber risk
- Present where you stand relative to industry benchmark and what is will take to move the needle to the average.
- Present all the areas where no progress will be made as well as areas not covered as part of your current operational design
- Provide resource and budget baseline relative to the industry average and size of your organization