10 Things to Consider

Before Buying a Security & Privacy Education Solution

Potentia
concepts

Digital Transformation, cloud computing and mobile devices are dramatically changing the way we work and with whom we work. With increased performance and convenience comes greater exposure to security threats, especially those directed at humans via laptops, mobile devices, email and social engineering.

Meanwhile, in the last few years we've seen new government regulations related to data privacy, notably – the European Union's General Data Protection Regulation (GDPR) launched May 2018 and the California Consumer Privacy Act (CCPA) launching January 2020. These and other industry standards such as ISO 27001 and Payment Card Industry Data Security Standard (PCI-DSS) all call for some level of workforce security awareness training and reporting.

Companies have had to shift gears quickly to adapt to changing technology trends and build training programs that allow them to demonstrate compliance and mitigate the risk without compromising performance and worker usability. Legacy training methods such as classroom and using PowerPoint slides are often out of date, not scalable, hard to track and not engaging to users. We believe that auditors and cybersecurity insurance brokers will be stricter in the future when requesting evidence of compliance and reporting progress. "Prep-Kits" and simply showing that courses exist will not be sufficient. Companies should demonstrate evidence of adequate subject matter coverage and that a significant percentage of their workforce has completed annual training and passed assessments with a reasonable passing score.

While compliance requirements may be similar, your training needs are certainly not. Factors such as company size, culture, industry, region, language, available training platforms, program maturity and budget are all factors which should be considered before buying your next security and privacy awareness education solution.

Let’s review 10 things you should consider before buying a Security & Privacy Education Solution

1 Deep Content Library

With constantly changing technology and workplace trends such as cloud computing, distributed teams, remote teleworking and use of both corporate and personal (BYOD) devices, does your workforce and diverse IT community have access to the topics and tools it needs to stay up to date?

Do training courses exist which allow your company to meet regulatory compliance and mitigate risk from cybersecurity threats and human error? Is your courseware aligned with your company culture, strategy and HR/IT policies which should be reviewed and updated on an annual basis?

Next, we believe that security and privacy courses are complementary topics which are better integrated into the same education program. It’s important to not only explain industry and regulatory rules (ex. GDPR, HIPAA, ISO) but also how they should be implemented into roles and daily operations. For example, staff in the HR department should learn record keeping and document classification. Security best practices such proper password management, multi-factor authentication, social engineering awareness, secure email and use of cloud tools are all related! Users should know what to do and who to contact when they suspect a privacy mistake, data breach or insider threat.

Finally, content should be engaging and relevant. Your program should have courses which are general and role-based. It should be adaptable to individual changing needs. Courseware with audio, text and gamification make information more engaging and help change culture and user behaviors over time. Using these three communication modalities allows users to learn at their own pace leveraging the modality that best resonates with them at that time.

Choose a vendor that can offer content depth and avoid running multiple siloed, fragmented and expensive education programs.

2 Modular & Bespoke

The fast food chain Burger King has a 40-year-old slogan “Have it Your Way”. That works well for customizing burgers but is also nice when designing your security and privacy workforce education. Some companies, typically smaller ones like to buy a pre-packaged “Happy Meal” (yes, another burger reference) while larger companies with more requirements want to design their own.

Regardless of your needs, it’s nice to have the option to purchase pre-designed courses or build your own tailored program and then customize the course with your company’s logo and branding. Do you want 2 35-minute courses, or 7 10-minute mini courses delivered over the course of the year. You decide what works best for your users and how security, privacy and compliance are integrated into a company-wide training plan. The ability to create development tracks is a helpful way to assign a custom curriculum to teams, specific roles and regional offices where users can take course at their own pace under a set schedule.

The best education vendors will give customers the opportunity to integrate company policies and support contacts into the courseware. They will allow customization of course functionality compliant to the Shareable Content Object Reference Model (SCORM) and recognized by most Learning Management Systems (LMS). For example, you should have the ability to control text and voice, add knowledge reviews, course final assessment questions, control passing score and choose to activate Linear Progression – a setting which controls if users can advance through course pages before they’ve competed the exercises.

3 Cloud-Based & Interoperable

Some companies call themselves “Born in the Cloud”, we’re still waiting for the band that does a Bruce Springsteen spin on this. This may involve your products and your vendors. Many are going through digital transformation migrating to cloud services over time and have a hybrid of cloud and legacy applications. Larger organizations may have training departments with multiple vendors, departments, global offices and subsidiaries running their own solutions.

Whichever your environment, choose a vendor that offers flexibility and can best support your platform, integration and consolidation needs over time. This means that the vendor can support 3 possibilities: (1) Run your program from your vendor’s LMS in the cloud; (2) Use a your own in-house LMS which may be in the cloud or on-premise; and (3) A hybrid solution using the vendors content and LMS and leveraging software APIs to exchange learner, course and report data. We will get to reporting capabilities in #5 – Robust Reporting.

4 Planning & Assessment

Do you want to add a turbo charger to your awareness program, drive culture change and impress your management? Start with a good strategy and plan.

There’s more at the end of this report but here are some quick tips:

- Figure out who needs to learn what
- Coordinate your program and any simulations with HR & Training
- Determine metrics and how you want to measure progress
- Take a baseline measure of the program & user knowledge
- Collect all your reporting requirements (CISO, DPO, HR)
- Organize communication, campaigns and reinforcement tools

5 Robust Reporting

Companies have their own tools and preferences for running reports. In the case of an LMS and training programs, the most common reports are user registration and course completion records. You need to know who's registered, a time stamp of when they took their required courses, their assessment score if one exists and if they passed.

When reviewing vendor reporting capability, you want flexibility and depth. There should be pre-made canned reports as well as the ability to build custom reports and schedule them for delivery to any individual in the organization. You'll want the ability to dump data into a spreadsheet, to analyze it or port it to another company reporting system as needed.

With regard to GDPR and other data privacy regulations, check with your data privacy and compliance officer on reporting and operating requirements. LMS administrators should minimize storing or transferring data files with personal information. Disable users purged from the user database should be tracked for proof of deletion.

6 Flexible Administration

Fancy dashboards are nice but does the solution should support your organization’s regional requirements and workforce structure.
Make sure that you can create groups or teams in your LMS and that information you need for each learner can be stored in the user database. The ability to create custom fields as needed is also key. An example of this is setting a Learner’s language preference.

A good LMS will also allow you to restrict access to fields in the user profile so they cannot be changed during or after self-registration. We’ve experienced how running reports by department can be a total nightmare when users have a myriad of different descriptions for their department, job title, etc. Batch load user profile details and lockout these fields. Only allow users update their password and contact numbers.

While on the topic of batch loading, this is a “must have” feature managing an LMS. You need the ability to load your user population, team and assigned courses and development tracks during implementation and then to maintain the database over time.

Privacy regulations such as EU GDPR state that users have the “Right to Be Forgotten”. If you are working under the jurisdiction of GDPR you will want to verify that your vendor can support the automatic purge of your LMS user database records that have been marked Disabled over a period of time to be decided by your company data privacy and compliance officer.

7 Multi-Language Support

Multi-language support is critical for customers that require a solution in their local language or to support offices, workforce and partners globally. Companies may want to centralize management of their content and platform and have the ability to launch the same program to everyone in their preferred language mix. They may want text and voice in the same language or choose a mix of voice (ex. English) with second language presented in subtitles.

When thinking about multi-language support here are the things from experience that we would consider in your vendor research:

- What's the depth of languages for courses that are pre-translated? Are the languages you need supported?

- Can the vendor provide custom translations for languages that are not supported? Can custom emails be sent from the LMS to learners running a custom, non-standard languages for things like registration, course invitations or password resets?

- Are the courses and LMS multi-language compatible, can you select a language preference for each learner?

- Does the vendor have attractive pricing for bundling multiple languages?

8 Simulations & Phishing

Phishing scams are a leading cybersecurity threat used to inject malware, ransomware or steal data by exploiting human behavior on their devices via email, social media and websites. Many companies are running email phishing simulations as a reinforcement exercise to complement learner training.

These tools exposes users to various phishing presentation styles and levels of sophistication and difficulty. Simulation is a great way to identify workers that need more support and education. It also allows your workforce, IT Security and Customer Support Team to practice standard procedures to identify, analyze and block malicious emails and then triage corrupted user devices.

Most security awareness vendors have a phishing simulator tool or a recommended partner. In this whitepaper, we don’t go deep into the evaluation of phishing simulators. Features of note include the ability for users to self-report suspected emails from their email box and to automatically enroll users into a short phishing course when they click on a link embedded in a phishing email also known as **“Taking the Bait”.**

9 Flexible Sales Packages

No one likes buying what they don't need and having licenses sit on the shelf. Make sure that your vendor's offerings fit your current needs and flexible enough for potential future needs. If you have a small company and all you need or have budget for is a "Happy Meal" then stick to that.

Some vendors offer worthwhile subscriptions to training packages that include courses, access to a cloud LMS and use of a phishing simulator. The ability to tailor your packaged courseware is a strong differentiator.

For large enterprise and global organizations, having the flexibility to buy subscription access to course catalogs across security, privacy and compliance and then custom tailor your courses, course duration and training track is a strong benefit. Enterprise level packages may include bundled support for an LMS, reinforcement materials, simulators and multiple languages.

Finally, don't be wooed by gadgets and marketing gimmicks, these are for tradeshows and for your engineers to play with. If they are not intended for production, then take this brain clutter off your decision-making table.

10 Experience & Support

When selecting a vendor, you need to consider more than functionality and the cost of licenses. Here are some areas to investigate:

Does the vendor have hands-on experience implementing security, privacy and compliance programs in your industry?

Does the vendor have knowledge of program design, operational best practices, program maturity and benchmarking?

Ask about the vendor’s support policy. Does it have qualified partners and customer relationship managers? How long does it take to get a response for a support call?

Ask for client references, read their blogs and whitepapers – are they a solid subject matter expert and thought leader?

Investigate financial health, corporate status and news releases. Is there activity that may impact your future ability to get desired service levels?

Conclusion

How to Plan and Use This Document

We wish you success in finding a security, privacy and compliance education vendor that meets your needs. For review, here are some questions you may consider before starting the evaluation process:

- Who do we need to train (ex. employees, contractors, partners)?
- List our industry and government regulatory compliance requirements
- Gather historical feedback from IT, CISO, CIO, customer care, HR and your privacy officer – past breaches, data leakage, policy abuse
- Organization structure, M&A, new office locations, teams, partners
- New product, services and technology tools
- Multi-language requirements, new offices and regions
- Program maturity, centralization, management, other training
- Workforce knowledge, assessment & culture
- Learning management system (LMS) – have or need
- Reporting, data consolidation & export requirements
- Customized program structure: long courses or short monthly ones
- Does your company have a training department and coordinator?
- Company size and deployment – Large enterprise, mid-size, SMB
- Vendor support – "We need help!" or "Leave us alone, we got this!"
- What's your budget? Single or multi-year contract possible?

The Evaluation

Indeed, one size does not fit all. Once you set goals and answer some guiding questions, we suggest prioritizing the 10 areas with a numeric weight of your choice. Score your vendors for each area (ex. 1-5), multiply each score by the weight and calculate a total quantitative score.

On the qualitative side, talk to vendors to get a feel for their culture, ask for references, read reviews and consider the stability of the vendor. Combine qualitative with quantitative and always **follow your gut!**

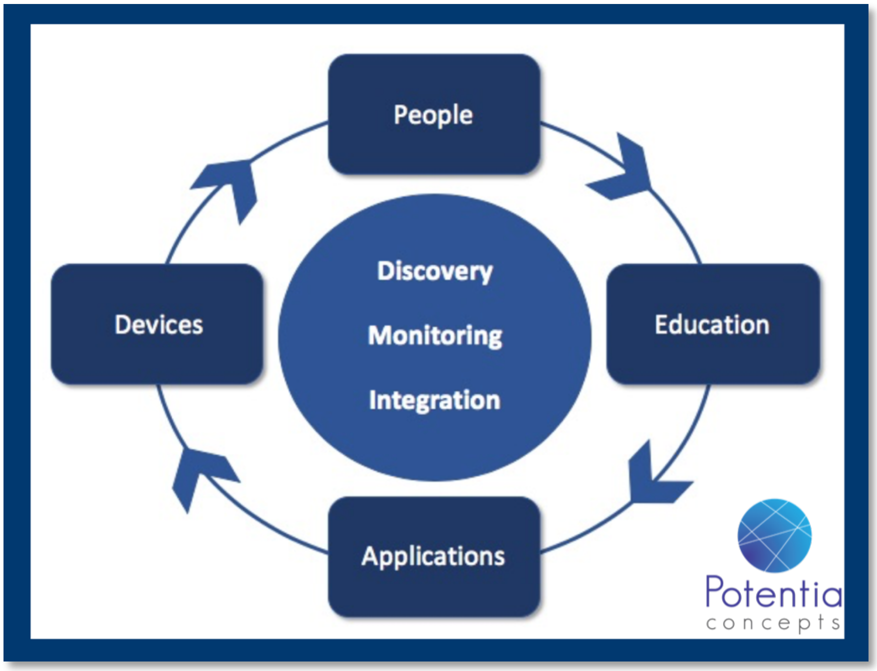
What is Human Factor Control and Enablement (HFCE)?

Human resources are your strongest asset but can also be your weakest link. When building your “zero-trust” and “defense in depth” environment it important to integrate OSI “Layer-8 – People”.

HFCE is a program developed by Potentia Concepts to help organization strengthen their security and privacy posture and mitigate risk with Human Factors.

HFCE phase -1 starts with workforce discovery and assessment of an organization’s IT user ecosystem, user security knowledge, learning program maturity and development of a new education awareness program

In HFCE phase-2 we re-discover corporate and user devices, IT applications and implement a new IT Access Management strategy.



Adam Hoey is CEO and Founder of Potentia Concepts with offices in Washington DC and Amsterdam, The Netherlands.

When he’s not riding a bike, Adam writes on topics related to digital innovation, product strategy, mobility, privacy and human-factor security.

He can be found at:
Potentia Concepts
Linked In

Contact Us
Amsterdam | Washington DC
www.potentiaconcepts.com
info@potentiaconcepts.com