Asia Perspectives

INTUITION

NOV 2019 - VOLUME I

Why are companies failing to reduce organizational cyber risk?

Here is why:

INTUITION PUBLISHING PTE LIMITED

Almost every industry is being disrupted by the 4.0 effect, there will possibly be implications of this rapid transformation that we cannot foresee. The ever-increasing drive to digitize the way we do business is completely changing business models. Long gone are the days of traditional bricks & mortar establishments and paper. Today's modern disruptors are more akin to I.T. service providers.

But are the cracks in this rapid transformation starting to show? We are reaching a point where the available talent to secure this transformation is running thin, I.T. Security spending may be reaching a celling. Global data privacy regulations are increasing, as the frequency and cost of breaches continue to rise.

One area there appears to be a disconnect, is between I.T. who take responsibility for hardware and software, and HR who take responsibility for people.

The sentiment often feel from I.T. is if they keep spending on better technology then they can mitigate errors caused by users. Likewise, HR often feel if a user makes an error then it's I.T.'s problem because the system has allowed the error to occur.

We really need to break down these departmental silos' and see a shared responsibility. What is good for the goose is good for the gander, or however that saying goes. If they both focus more on the people and raise their awareness, skills and culture, they will reduce overall risk, at a time when it could be crucial to the survival of the business.

60% of Small Businesses fold within 6 months of a Cyber Attack.

Sometimes it's easier to justify the cost of a new security tool that shows documented benefits, rather than spending on further employee training, that if not delivered correctly can be difficult to measure the impact to risk reduction. It must be noted the vast majority of breaches are still attributed to employee error, weather that be from operational errors such as leaving and open database on the internet containing sensitive customer information, or social engineering tricks to exfiltrate intellectual property.

So why are we not focusing more efforts on employee training and awareness?

Up-to 90% of all data breaches are caused by human error. Not technical infiltration.

In many of these cases, the companies have spent huge amounts on cyber security hardware and software but failed to realize cyber security does not stop at the workstation.

Computer systems have come a long way in recent times, and now they are quite reliable, the computer will do as it is programmed. The component that has been slower to evolve is the biological one operating the computer. Humans often do not do as they are programmed, they have off days and can be tricked into doing things they should not. They even have tendencies to knowingly take risks influenced by their environmental culture.

Fortunately, there is now a very rich field of academic study on behavioral psychology and understanding how people learn, and why they take certain risks knowing they should not. When combined with advances in Data Science and Machine Learning it is possible to overcome the aforementioned problems in measuring the impact of risk reduction.

By designing a cyber security training and awareness platform from the ground up, based entirely on widely accepted behavioral science theories, and using ML to personalize the content and delivery to each individual's preferences, it is no longer a guessing game. You can actually demonstrate an increase in awareness and skills, an improvement to security culture and attitudes, and ultimately an overall reduction in risk posed by employees.

We all know that many business operations are driven by data and the insights that can be derived from such data. To be operating in today's environment without data on your employees and the risks they may pose to your organization seems ludicrous. Yet many are still only meeting the baseline of compliance-based tick box awareness.

Your employees present a vast attack surface for an adversary, with a continual churn. If I want to penetrate a company my first point of contact will be the employees not the network. In the fight against ever increasing threats your employees can be your greatest asset or your weakest link, it's up to you how you train and monitor their level of awareness and your security culture.

Contact us for more information on how Intuition can help implement a Cyber Security training, an intelligent cyber security awareness, behavior and culture platform

Get the app

Intuition-Know How

The Intuition Know-How Library consists several tutorials related to this article:

- **Cyber Security Awareness (GCHQ-UK Certified Training)**
  - Passphrases
  - Preventing Identity Theft
  - Device Security
  - Malware & Breach Recovery
  - Social Engineering
  - And More…
- **Operational Risk Management**
  - Operational Risk - An Introduction
  - Operational Risk - Measurement & Reporting
  - Operational Risk Management - Tools & Techniques
  - Operational Risk Management - Developments & Emerging Risks
- **Global Financial Regulation**
  - Financial Regulation - An Introduction
  - Financial Authorities (Japan)
  - Financial Authorities (Hong Kong)
  - Financial Authorities (Singapore)
  - Financial Authorities (China)
  - And More….

For Intuition blended learning related to this article, some of our popular workshops include:

- Introduction to and Overview of Risk Management in Banks
- The Human weakness – Social engineering
- Evolution of 2FA - Strong Customer Authentication – RTS PSD2 SCA with FIDO2

The topics covered in Intuition Asia Perspectives are current developments or topics currently in the market. Intuition Asia provides bespoke learning solutions, both eLearning and Instructor-led courses. These can also be blended in a program to provide the most effective form of learning. These workshops can be structured as lunch & learns, webinars or full day deliveries. Clients can use these to keep their workforce updated with the latest developments in the market and complete their mandatory CPD learning hours.
Get in touch with your Intuition account manager at apacinfo@intuition.com for more details

Related News Articles

- *The Cybersecurity Talent Gap = an Industry Crisis-Security Magazine-30 Apr 2019*
- *Sensitive data is widespread in digital transformation environments -Thales-2019*