CyberEx Academy

Cyber Risk Training for Everyone!

Cyber Risk Management Simulations

We use our unique, multi-patented cyber risk management software solutions to provide your personnel with hands-on experiential learning within a safe environment.

Cyber risk simulations are the bridge between traditional modes of teaching and on the job, real life operations. Our software facilitates understanding of all aspects of cyber risks, your organisations specificities and how they relate to cyber exposure and how it can be managed.

Through cyber risk management simulations your team members will:

- Develop an understanding of the factors affecting exposure
- Use hands-on learning to build cyber knowledge and skills
- Determine which systems or processes are at most risk
- Comprehend risk transfer options
- Calculate cost-benefit option effectiveness

Learning experientially leads to your teams' ability to meaningfully contribute in all discussions relating to cyber risk exposure.

Understanding of factors affecting cyber exposure leads to development of resilience through taking strategic decisions in relation to IT security investment, IT general controls testing, fit to overall enterprise risk management, feeds in to business continuity planning and a broader set of IT and cyber risk control operations.

Leading corporations use business simulations to improve performance in all aspects of their business. We can add to your existing programmes and add cyber risk control capabilities to your organisation.

Cyber Risk Awareness Training

Amended and new regulations in the UK, EU and US now mandate cyber awareness training, for all levels of personnel, with the burden of proof of training falling to every organization. As with many data privacy regulations, it is for companies to prove they are compliant with auditable proof.

CyberEx assists your organization through the provision of verifiable evidence of training, whether we deliver this in-person or remotely. Our objective is to ensure we deliver effective cyber awareness training in a manner enabling your staff to retain their newly acquired knowledge and use it in practice within their roles.

- Regulations & updated standards for 2022 require cyber awareness training at all levels within organisations

WHAT-IF SCENARIOS

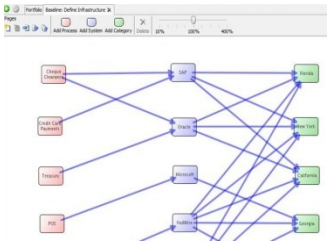
- Ability to create multiple scenarios and measure against baseline financial and operating risk exposures

Scenarios

Name	Implementation Cost ($K)	N-Opvar ($K)	Saving ($K)
Baseline	0.0	114,642,143.4	0.0
Increased CCT...	1,237,890.0	292,818,682.5	-179,414,429.1
New Door Locks	20,000.0	17,957,289.5	96,664,854.0
Weather Warni...	300,000.0	71,801,715.6	42,540,427.9
Additional Physi...	500,000.0	77,503,546.0	36,638,597.4
Increased IT S...	12,000,000.0	21,138,127.8	81,504,015.6

HANDS-ON EXPERIENCE

- Test mitigation actions on a cost-effective basis to target capital spending for enhanced cyber resilience



CROSS-FUNCTIONAL BENEFITS

- Facilitates collaborative working within your organisation, reducing cyber risk exposure, building cyber operational resilience

- People change roles. Having an internal network to draw upon results in continued contact points for valuable cyber risk management insights
- Shared learning – different company participant profiles create a shared experience that continues post-training
- Don't take a whack-a-mole approach to your cyber risk management strategy
- A cyber-attack on your client, competitor, or supplier is a great motivator – be proactive and manage your cyber risks effectively
- If you do not show your people what they should, or should not do, how can you expect them to fulfil your expectations?

Technology Risk Management Training

Technology risk management extends beyond cyber risk management and focuses more upon operational factors that can impact upon an organizations' technology function. Of major importance to external auditors, information technology general control effectiveness (ITGC's) impacts heavily upon your organization in terms of time and cost.

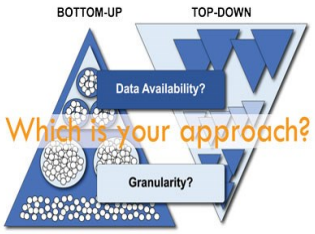
Where ITGC's are found to be deficient, or where a cyber attack has successfully breached perimeter defences, your next statutory external audit and those in following periods, will take considerably longer due to a greater degree of examination of control design, applicability and operation by auditors. The costs of prolonged ITGC and associated technology risk controls can be considerable and not limited to purely the next audit period.

Our training targets the IT general control (ITGC) and financial statement line item impact (FSLI) areas of risk control.

- Identify and assess IT general controls
- Provide input to internal and external IT audit teams
- Meet increasing regulatory and standards training mandates
- Increase overall cyber resilience
- Up-skill non-technical managers for the future
- Create and maintain cyber risk frameworks
- Satisfy external auditors – high ITGC performance
- Define future IT risk controls with broader user inputs
- Create alignment of IT with corporate risk management strategy

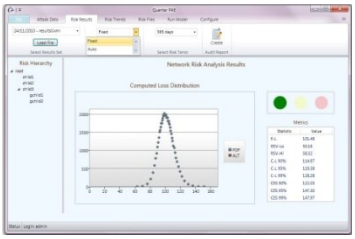
CORE MODULES

- Includes psychology in decision making, risk management, technology functions, risk management, situational awareness.



TARGET GROUPS

- Awareness: All levels
  Cyber: Managerial/execs
  Tech: Managerial



TEACHING METHOD

- Blended learning using traditional and experiential learning based upon our 25 years of teaching experience

DELIVERY TIMES

- Our modular approach enables us to deliver in a maximum of one day

CyberEx Academy