HARVARD
Office of the Vice Provost for Advances in Learning

CYBERSECURITY:

MANAGING RISK IN THE INFORMATION AGE

ONLINE SHORT COURSE

Lead the strategic response to cyber risk.

HARVARD
Office of the Vice Provost for Advances in Learning

HarvardX

ABOUT THIS COURSE

News of large-scale cybersecurity threats and cyberattacks dominate the headlines all too often in today's Information Age: hackers exploiting vulnerabilities of a retail giant, foreign influence in elections, and new forms of ransomware underscore the importance of preparing for these types of emerging threats. As businesses, governments, financial institutions, and public sector organizations collect, store, and process vast amounts of sensitive and valuable data, those organizations become targets of groups seeking to wreak havoc on vulnerable systems and potentially disrupting everyday business functions. As a result, cyber risk management has become a fundamental component of business operations, and understanding and mitigating risk has become an essential skill for business leaders, thought leaders, analysts, as well as security and technology specialists.

Harvard VPAL's *Cybersecurity: Managing Risk in the Information Age* is an online short course that equips students with a comprehensive understanding of how to identify and manage operational risk, litigation risk and reputational risk. The course will help students assess and mitigate specific vulnerabilities within an organization's networks, systems, and data in order to provide the knowledge and skills to protect the integrity, security, and confidentiality of their digital assets.

8 weeks, excluding
1 week orientation

8 - 11 hours/week
of self-paced learning,
entirely online

$2,800
Installment options available
Tax may be charged on the course fee depending on your country of residence

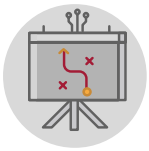
Spending on cybersecurity in the United States is projected to reach **$66 billion in 2018.**

**Telecommunications Industry Association (USA)*

WHAT THE COURSE COVERS

You'll be shown how to critically analyze an organization's risk profile, not only taking into account possible threats, but also the governance structure and systems that have, or have not, been put in place to manage cyber risk. You'll also explore recommended strategies for responding to a cyberattack, starting with identifying and communicating detection of a security breach, to ensuring that the attack is contained to prevent further damage. The course will also draw your attention to the legal and compliance regulations that ensure organizations remain compliant with both preventative and reporting requirements. At the end of the course, you'll have developed the appropriate knowledge to design and successfully implement a risk mitigation strategy for an organization.

THIS COURSE IS FOR YOU IF:



You want to lead an organization through the complexities of risk management in the current cybersecurity landscape

You have a goal to understand the impact of cyber risk on an organization's capacity to accomplish its stated mission

You'd benefit from recognition of your understanding or specialization in the field of cyber risk management

I want professionals to come away from this course prepared to take a strong leadership role in improving the cyber risk management within their own organizations. Based on my experience as a CISO and the leader of cyber issues at the Department of Defense, I want this course to help you answer the toughest questions: What are my organization's most important assets and how can we mitigate the risk of attack to them? When a cyberattack attack occurs, how can we implement a response plan that minimizes operational, litigation, financial, and reputational risks?

— ERIC ROSENBACH

Course Convener, Co-Director, Belfer Center for Science and International Affairs, Harvard Kennedy School

WHO SHOULD TAKE THIS COURSE?

This course is designed for leaders at all levels who must pilot their organization through the complexity of a dynamic cybersecurity environment and mobilize appropriate resources to maintain stable business operations. This course is also invaluable to technology specialists aspiring to a leadership role, as well as security experts who need to upskill in such a rapidly evolving field. Additionally, thought leaders, management professionals, analysts and technical writers who must interpret and communicate the implications of cyber threats to stakeholders will benefit from this online professional development experience.

WHAT YOU'LL LEARN

This online short course integrates rich, interactive media such as videos, infographics, and e-learning activities as well as traditional didactic components such as written study guides (course notes). There are also opportunities for collaborative learning through discussion forums. The following modules contribute to the holistic approach your learning path takes:

ORIENTATION MODULE

ONE WEEK

WELCOME TO YOUR ONLINE CAMPUS

You'll be welcomed with a personal call and get introduced to your online teaching and technical support network. Begin connecting with fellow students while exploring the navigation and tools of your Online Campus. Be alerted to key milestones in the learning path, and review how your results will be calculated and distributed.

You'll be required to complete your student profile, confirm your certificate delivery address, and submit a digital copy of your passport/identity document.

MODULE 1

CYBERSECURITY RISK IS BUSINESS RISK

Explore the concept of risk management frameworks that help ensure an organization's cybersecurity. Module 1 introduces six noteworthy cases of security breaches that highlight the risk of insecure information systems and the importance of implementing adequate risk management frameworks. These cases are drawn on throughout the course to bolster theory with tangible examples. The second half of the module will discuss operational business risk, litigation risk, and reputational risk.

MODULE 2

IDENTIFYING THE THREATS TO AN ORGANIZATION

Investigate the threats to an organization's critical business systems and data by understanding the sources of pertinent cybersecurity threat actors and the methods commonly used to infiltrate an organization's security systems. Explore three types of threat actors, namely nation states, cybercriminals, and internal organizational threats, including the methods they are likely to employ, and the types of organizations or sectors they typically attack.

Begin work on an ongoing real-world application project that will conclude in Module 8 by analyzing the vulnerabilities of your own organization to identify potential threats posed by nation states, cybercriminals, and insiders. Alternatively, students can choose to complete their project using a case study of the Sony Pictures hack of 2014.

MODULE 3

IDENTIFYING IMPORTANT BUSINESS SYSTEMS AND ASSETS

Identify internal assets and business critical systems (BCSs) that need to be protected from cyberattack if an organization is to function effectively and efficiently. Explore the degree of risk in relation to an organization's systems, networks, and data. Gain foundational knowledge to better evaluate and understand the implications on internal processes, and how these assets and systems should be protected. Using a chosen organization, or the case study provided, identify BCSs that are affected when the integrity of an organization's systems, networks, and data are compromised, and describe how the interruption caused by an attack affects its capability to perform everyday functions.

COURSE COMPLETION RATE

Achieved through a people-driven support model of online learning, tailored to individual needs.

MODULE 4

THE CRUCIAL ROLE OF LEADERSHIP IN MANAGING CYBER RISK

Understand the role of leadership in ensuring an organization maintains an effective strategy for keeping its cybersecurity systems up-to-date, and learn to identify stakeholders in the leadership and governance structure of an organization who play a key role in managing cybersecurity. Learn how to assess whether sufficient management processes have been put in place to mitigate the risk of cyberattack. Invoke a sense of appreciation in others for security awareness and training, and design best practices for implementing a training program in an organization. As part of your ongoing project, develop a cybersecurity leadership plan that considers effective management processes to mitigate cyber threats, either for your own organization or for the case study provided.

MODULE 5

UNDERSTANDING YOUR TECHNOLOGY

Examine the importance of implementing appropriate technologies to mitigate the risk of cyber threats. Understand how to recommend technologies to secure the three key dimensions of an organization's cybersecurity, namely the system, the network, and crucial data. You'll be assessed on your understanding of how an organization's systems, networks, and data interconnect and the various methods of attack and countermeasures in relation to each dimension. You'll also be required to identify appropriate technologies for managing the cyber safety of these three elements.

MODULE 6

CYBER RISK AND THE LAW

Navigate one of the most complex aspects of managing cyber risk, namely legal and compliance considerations at a state, national, and international level. Identify the impact of failing to take legal and compliance considerations into account and explore the requirements of your own organization's sector while learning to ask appropriate questions that assess an organization's adherence to these legal and compliance requirements.

How do we create online learning experiences that truly allow learners to achieve more? We are excited to announce a new kind of development experience that will lead to more impactful and significant learning outcomes. This is done by bringing together University expertise, the best of digital learning and higher-touch human learning, through an exciting collaboration with GetSmarter.

— PROF. ROBERT A. LUE, FACULTY DIRECTOR OF HARVARDX

MODULE 7

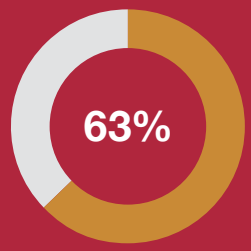
INCIDENT RESPONSE AND ACCOUNTABILITY

Learn the appropriate response to a breach in an organization's cybersecurity. The module focuses on three phases of a security breach, namely detection of the breach, communication of the breach, and containment of the breach. In each of the three phases, you'll be provided with an overview of the roles played by notable actors, and the processes that need to be implemented to mitigate any damage caused by a cybersecurity breach. As part of your ongoing project, you'll be required to propose an effective incident response plan that addresses a cybersecurity breach. This includes describing proactive measures for how you would detect the breach, the chain of communication that would be followed, and strategies for containing the breach to avoid further damage.

MODULE 8

DESIGNING AND IMPLEMENTING A MITIGATION STRATEGY

Understand the critical focal points that should be included in an effective mitigation strategy, while further exploring topics such as the implications around implementation, the allocation of financial resources, and establishing an accurate metrics system to keep track of the security systems that have been put in place. Module 8 concludes with a discussion that explores the future direction of cybersecurity, particularly in light of the evolving landscapes of artificial intelligence, big data, and geolocational data, and the increased organizational risks that accompany these advances. In the final aspect of your ongoing project, you'll bring together the knowledge you have gained in all preceding modules to design a risk mitigation strategy for your own organization, or continue with the case study provided.



OF OVER 1,000 SURVEY RESPONDENTS
deem it very important for data security professionals in organizations who have access to personal information to hold a cybersecurity certification.

WHO YOU'LL LEARN FROM

YOUR COURSE CONVENER

This subject matter expert from Harvard Kennedy School guides the course design and appears in a number of course videos, along with a variety of cybersecurity professionals

ERIC ROSENBACH

Course Convener, Co-Director, Belfer Center for Science and International Affairs, Harvard Kennedy School

As the Chief of Staff to Secretary of Defense Ash Carter from 2015-2017, Eric Rosenbach was one of the senior-most leaders of an organization with 2.8 million personnel, a $585 billion annual budget and ongoing military operations in multiple locations around the world.

Rosenbach was charged with managing some of the Department's most sensitive decisions and ensuring implementation of transformative changes in the Department's technology, budget, and talent management. He served as the Secretary's closest strategic advisor on the war strategy and global coalition to defeat ISIS, the "rebalance" to Asia, and the effort to check Russian aggression. Rosenbach also led the Department's efforts to improve innovation by forging and managing key initiatives such as the Defense Digital Service, the Silicon Valley-based Defense Innovation Unit and the Defense Innovation Board.

Before serving as Chief of Staff, Rosenbach was the Assistant Secretary of Defense, confirmed by the U.S. Senate, responsible for leading all aspects of the Department's cyber strategy, policy, and operations. His diverse portfolio as Assistant Secretary also included countering the proliferation of weapons of mass destruction, space operations, antiterrorism, continuity of government and defense support to civil authorities. Rosenbach led the Department's efforts to counter cyberattacks by Iran and North Korea on US critical infrastructure and deter Chinese theft of American firms' intellectual property.

Earlier, Rosenbach worked at the Harvard Kennedy School as the Executive Director for Research at the Belfer Center for Science and International Affairs. In addition to running the Center, Rosenbach taught graduate-level classes in cyber- and counterterrorism. Prior to his work at Harvard, he served as National Security Advisor for then Senator Chuck Hagel and as a professional staff member on the Senate Select Committee on Intelligence where he led oversight of Intelligence Community counterterrorism programs.

Rosenbach also has significant experience in the private sector, where he led the cybersecurity practice of a global management consulting firm, advising the executives of Fortune 500 companies on strategic risk mitigation strategies. Earlier in his career, he worked as the Chief Security Officer for Tiscali, the largest pan-European internet service provider, where he was responsible for all aspects of the firm's cybersecurity.

A former Army intelligence officer and Commander of a telecommunications intelligence unit, Rosenbach led a team that worked closely with the NSA to provide strategic intelligence in direct support of commanders in Bosnia and Kosovo. The Director of Central Intelligence named Rosenbach's unit as the top intelligence organization in the U.S. military for two consecutive years.

Rosenbach has authored many books and contributed articles on national security issues to the *New York Times*, *Washington Post*, and *Boston Globe*. The *LA Times* called his book, *Find, Fix, Finish*, co-authored with Aki Peritz, "an important volume in the secret history of a nasty war." He was a Fulbright Scholar and holds a Juris Doctor from Georgetown, Master's of Public Policy from the Harvard Kennedy School, and Bachelor of Arts from Davidson College.

HOW YOU'LL LEARN

This course integrates rich, interactive media, traditional didactic components, and opportunities for collaborative learning, to deliver a high-engagement learning experience:

- Work through your downloadable and online instructional material
- Interact with your peers and tutors through weekly class-wide forums and graded small group discussions
- Enjoy a wide range of interactive content, including video lectures, infographics, live polls, and more
- Investigate rich, real-world case studies
- Apply what you learn each week to quiz assessments and ongoing project submissions, culminating in the development of your own cyber risk mitigation strategy

TECHNICAL REQUIREMENTS

BASIC REQUIREMENTS

In order to complete a course, you will need a current email account and access to a computer and the internet. You should be familiar with using a computer and accessing the internet, as you may need to be able to read documents in Adobe PDF Reader, view Microsoft PowerPoint presentations, and read and create documents in Microsoft Word.

In addition, you will need to install Adobe Flash Player to view the video lectures, resources and activities available in each course module. Both Adobe applications are available for download:

Click here for Adobe Reader

Click here for Adobe Flash Player

BROWSER REQUIREMENTS

We recommend that you use Google Chrome as your internet browser when accessing the Online Campus. Although this is not a requirement, we have found that this browser performs best for ease of access to course material. This browser can be downloaded from the following website:

https://www.google.com/intl/en/chrome/browser/

ADDITIONAL REQUIREMENTS

Certain courses may require additional software and resources. These additional software and resource requirements will be communicated to you upon registration and/or at the beginning of the course. Please note that Google, Vimeo and Youtube may be used in our course delivery, and if these services are blocked in your jurisdiction, you may have difficulty in accessing course content. Please check with a course consultant before registering for this course if you have any concerns about this affecting your experience with the Online Campus.

YOUR SUCCESS TEAM

Harvard's Office of the Vice Provost for Advances in Learning, in association with HarvardX, are collaborating with GetSmarter to deliver this online professional development experience, that offers a highly-supported, personalized approach to online education.

HEAD TUTOR

A subject expert who'll guide you through content-related challenges

SUCCESS MANAGER

Your one-on-one support available during University hours to resolve technical and administrative challenges

GLOBAL SUCCESS TEAM

Available 24/7 to solve your tech-related and administrative queries and concerns

AN UNPRECEDENTED COLLABORATION

Harvard's Office of the Vice Provost for Advances in Learning and HarvardX are collaborating with online education company GetSmarter to create a new class of learning experience that is higher-touch, intimate and truly transformative. Prof Robert Lue, Faculty Director of HarvardX, believes that, in addition to a focus on the quality of content, an online learning model built on human mentorship and performance coaching, administrative and academic support, individualized assessment feedback and rich social interaction with peers, "leads to much more impactful and significant learning outcomes."

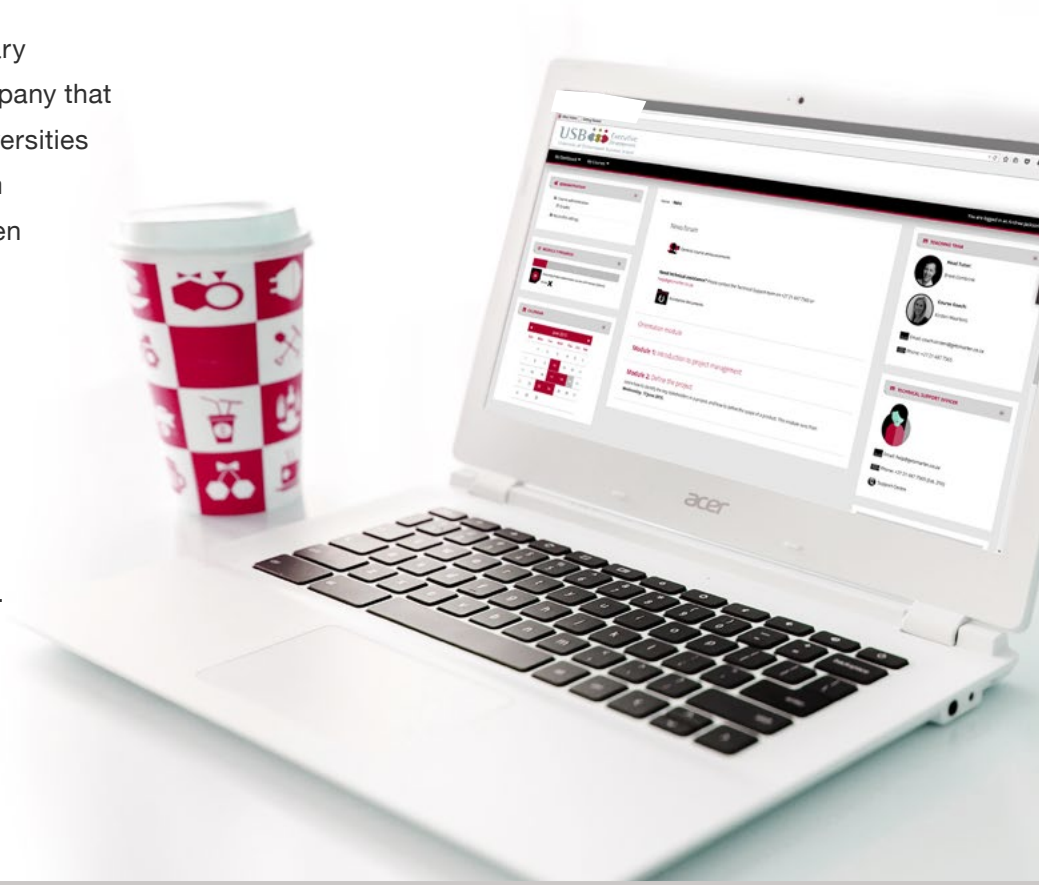
WHAT IS VPAL AND HARVARDX?

Harvard University's Office of the Vice Provost for Advances in Learning (VPAL) fosters the highest quality 21st century learning experiences, both on campus and online. HarvardX is the strategic online learning initiative overseen by VPAL, which since 2012 has brought the best of the University's various schools to learners across the world. With a focus on developing ever more innovative ways to support learning online, HarvardX's work with GetSmarter establishes a new standard for combining world-class content with a fully supported and high-touch experience.

WHAT IS GETSMARTER?

GetSmarter, a wholly-owned subsidiary of 2U, Inc., is a digital education company that partners with the world's leading universities to select, design and deliver premium online short courses with a data-driven focus on learning gain.

Technology meets academic rigour in our people-mediated model which enables lifelong learners across the globe to obtain industry-relevant skills that are certified by the world's most reputable academic institutions.



HARVARD
Office of the Vice Provost for Advances in Learning

CYBERSECURITY

MANAGING RISK IN THE INFORMATION AGE

ONLINE SHORT COURSE

Ready to lead the strategic response to cyber risk?

REGISTER NOW

CONTACT US

Email: registrations@getsmarter.com

Call: US: +1 224 249 3522 | UK: +44 20 3457 5774 | Global: +27 21 447 7565

www.getsmarter.com

HARVARD
Office of the Vice Provost for Advances in Learning

HarvardX