ADVANCED CYBERSECURITY PROGRAMME FOR LEADERS

10 WEEKS + ONLINE GIM NETWORK

LEARN FROM ONE OF THE TOP B-SCHOOL IN INDIA

INTEGRATED WITH GENERATIVE AI

IN COLLABORATION WITH

BlackPerl

Programme Overview

The global cybersecurity market is set to grow significantly—from **$183 billion** in **2024** to **$292 billion** by **2028**—driven by a rising wave of cyber threats impacting critical systems and services around the world. As these threats grow in scale and complexity, there is a soaring need for skilled cybersecurity leaders who can detect, prevent, and respond to attacks effectively.

In response to this urgent need, GIM has partnered with BlackPerl to launch the **Advanced Cybersecurity Program for Leaders**, a forward-looking initiative designed to equip professionals with the skills to lead in this evolving landscape. The program integrates cutting-edge topics like Artificial Intelligence (AI) and Generative AI, enabling participants to strengthen their organization's cyber resilience.

This intensive program offers a well-rounded curriculum that covers key areas such as cybersecurity governance, risk and compliance, and the strategic use of AI for smarter decision-making. It's designed to empower you with the knowledge and leadership capabilities needed to build strong cybersecurity teams and take on high-impact roles in the industry.

According to IBM's 2023 Cost of a Data Breach Report, the global average cost of a data breach reached **$4.45 million**—a **15% increase over three years**. Alarmingly, **51% of organizations are planning to increase security investments** in areas like incident response, threat detection, and employee training, indicating a growing urgency to mitigate risk.

Programme Summary

Institute Name
GIM

Duration
10 Weeks

Cost
INR 50,000 + GST

Learning Mode
Online

Weekly Effort
8 to 10 hours

Faculty
GIM Faculty

Industry Expert
Senior Industry Practitioner, C-Suits

Program Leader
Subject Matter Experts/ Mid-industry Practitioners

Eligibility
Any Graduate/ Diploma Holder

Certificate
Upon Successful Completion of the Programme, Participants Will Be Awarded a Verified Digital Certificate From GIM & BlackPerl

Live Class/ Instructor Led
Great the best learning experience, Nothing Is better than Live Class

Lifetime Recording Access
Re-watch any lesson/concept for deeper understanding

Co-Hort Based Learning
Networking and community interaction by using discussion boards

Gain Live Project Experience
Don’t only learn, apply them in Customer Project
Enhance your skills under Industry mentorship

Focus on Practicals
Learn by doing, the whole course is divided
By 70% practical experience

Industry Overview

As cybersecurity rises on the risk and leadership radar, **GIM** has launched the **Advanced Cybersecurity for Leaders programme** integrated with **AI** and **Generative AI** to help you safeguard your business against the escalating frequency and sophistication of cyber attacks. This strategic choice programme offers a pathway to a high-growth career as a cybersecurity leader by teaching you how to become proactive and versatile in this dynamic field.

Cybersecurity is no longer a choice but a strategic imperative for today's leaders. With the threat landscape becoming more complex and persistent, organizations are significantly ramping up their security investments. IDC reports that **global spending on security solutions—including software, hardware, and services—is expected to surpass $219 billion by 2024**, reflecting how central cybersecurity has become to long-term business resilience and risk management.

A recent analysis by McKinsey & Company highlights a significant acceleration in cybersecurity investment, with global spending on security products and services projected to grow at an **annual rate of 13% through 2025**. This marks a notable increase from the **10% average annual growth** seen over the past several years, reflecting how rapidly organizations are prioritizing cybersecurity in response to the evolving threat landscape and increased digital transformation efforts.

52%

OF PUBLIC ORGANISATIONS REPORT THAT SKILLS AND RESOURCING ARE THEIR BIGGEST CYBER RESILIENCE CHALLENGES.

56%

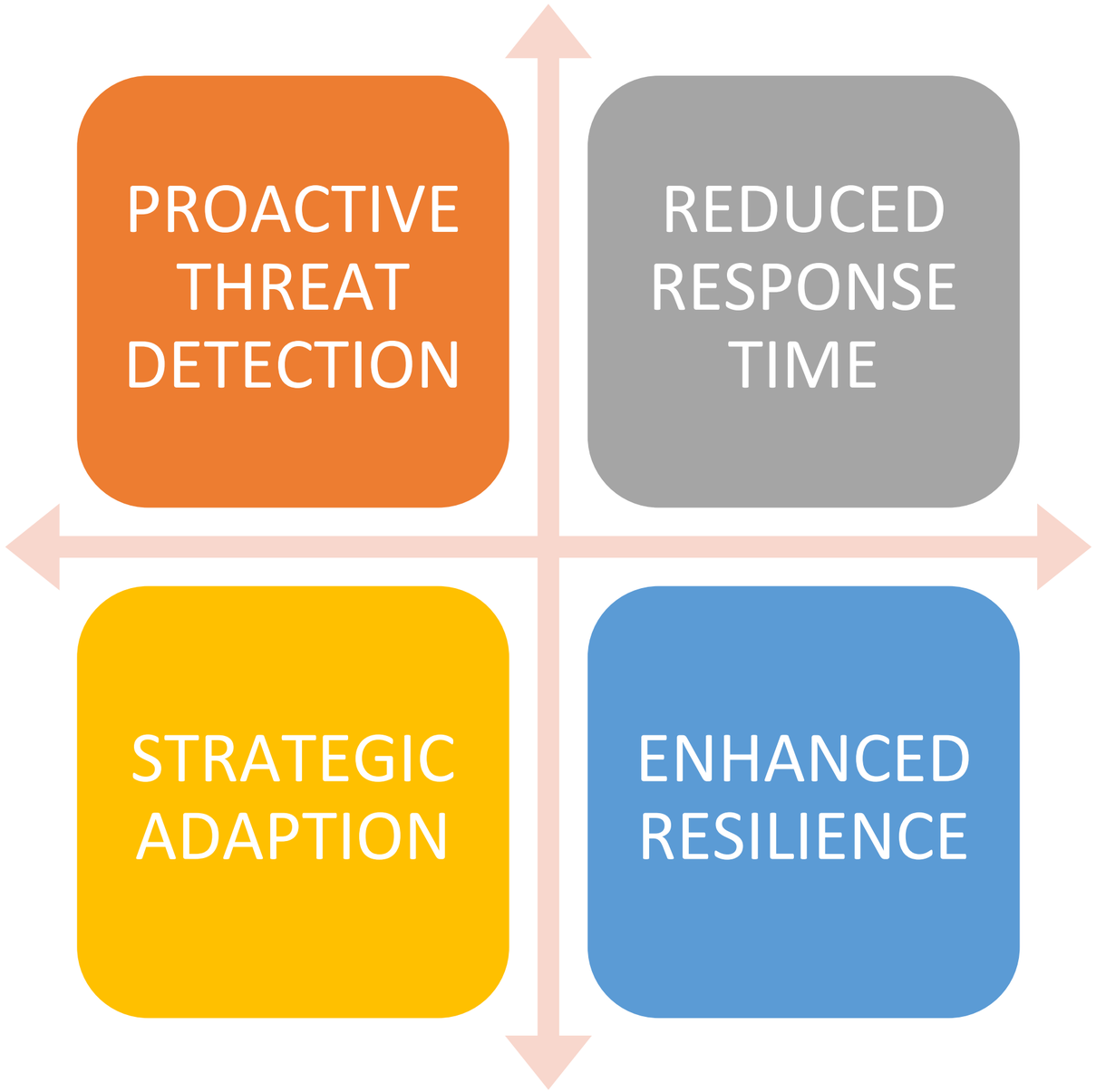
OF LEADERS BELIEVE GENERATIVE AI WILL ADVANTAGE CYBER ATTACKERS OVER DEFENDERS IN THE NEXT TWO YEARS.

31%

DROP IN ORGANISATIONS REPORTING A MINIMUM CYBER RESILIENCE SINCE 2022.

SOURCE: WORLD ECONOMIC FORUM, GLOBAL CYBERSECURITY OUTLOOK 2024

Impact of Emerging Technologies -AI & Cloud on Cybersec



Programme Highlight

Practical cybersecurity tools and technologies

Life-time Access to Recorded Materials

Live Interaction with Instructors And Mentors

Fire-Side Chat with Industry Body

Real-world case studies and business scenarios

1 Industry Visit

Assessments with real Project experience

Global Recognition, Access to Industry network

Real World Case Studies and Business usecases

Mashreq Bank Risk Management

Microsoft Cutting Edge Solution for Risk Mitigation

Aadhar Security Breach Analysis

Elastic Security AI Solution against Threat Detection

BlackPerl's Crisis Management

Cyber Security Tools and Technologies to be Covered

++Many more Opensource Industry Grade Products and Solutions

Programme Modules

Module-1

Introduction to Cybersecurity

- Information assets
- Cybersecurity risks and threats
- Information Security Management System (ISMS) Information Security
- Management Objectives: The CIA Triad How information security works
- Offensive and defensive strategies
- ISMS standards and compliance
- ISMS best practices
- Building a cybersecurity culture in an organisation
- Building a cybersecurity strategy

Module-2

& Python Scripting

Regulations and Compliance

- India’s cybersecurity laws and regulations
- The Information Technology (IT) Act, 2000 Computer Emergency Response Team (CERT-In) Information Technology (Amendment) Act 2008 Information technology rules, 2011
- Information technology rules, 2021
- Essential practices for cybersecurity professionals
- National Cyber Security Policy, 2013, National Cyber Security Strategy, 2020
- Digital India Act, 2023, Data protection laws in other countries
- National Critical Information Infrastructure Protection Center (NCIIPC) ISO/IEC 27001
- Know Your Customer (KYC)- Regulatory framework for financial and telecom sectors in India Risk assessment and mitigation strategies

Module-3

Security Strategy and IT Infrastructure

- Developing and implementing a cybersecurity strategy
- Writing effective security policies and procedures Security awareness and training programmes
- Budgeting for cybersecurity and team
- Evaluating risk exposure
- Cybersecurity control and operations, identifying threats

Programme Modules

Module-4

Ethical Hacking

- Introduction to Ethical Hacking & Legal Boundaries
- Information Gathering & Reconnaissance
- Scanning & Vulnerability Discovery
- Exploitation & Gaining Access
- Web Application Hacking Basics
- Post Exploitation, Reporting & Defense

Module-5

Cyber Security Emerging Trends

- **Overview of Cybersecurity Tools**: Firewalls, antivirus software, intrusion detection/prevention systems, and SIEM (Security Information and Event Management).
- **Emerging Technologies**: The role of AI, machine learning, blockchain, and quantum computing in cybersecurity.
- **Cybersecurity Metrics and Analytics**: Measuring and monitoring cybersecurity effectiveness.

Module-6

Business Continuity and Disaster Recovery

- Business Continuity and Disaster Recovery (BCDR) planning
- Benefits of Business Continuity and Disaster Recovery (BCDR)
- Activating Business Continuity and Disaster Recovery (BCDR)
- Common disaster recovery teams
- Disaster classification
- Disaster recovery process
- Elements of a disaster recovery plan
- Business continuity strategies
- Timing and sequence of planning activities Business continuity in scenarios of threat BCDR: Some common mistakes to avoid

Module-7

Ransomware and Malware Analysis

- Introduction to Malware Analysis.
- What is Ransomware and the trends of attacks of Ransomware
- Explore various types of malware and ransomware, how they spread, and ways to protect against them
- Gain hands-on experience in conducting malware analysis and incident response to detect and manage cyber threats effectively

Programme Modules

Module-8

Proactive Threat Detection, AI in Cybersecurity

- Introduction to Threat Detection
- Setting Up the Threat Hunting & Analytics Platform
- Data-Driven Threat Hunting with Python & Jupyter
- Advanced Threat Hunting with Machine Learning
- SIEM Integration with Jupyter — Elastic, Splunk & Azure Sentinel Notebooks

Module-9

Incident Response and Crisis Management

- Incident Response (IR): Overview Incident Response (IR): Process
- Incident Response life cycle
- The do’s and don’ts of Incident Response Incident handling scenario – Ransomware Incident handling scenario – Malware
- Incident handling scenario – Phishing Crisis management
- Crisis communication and public relations
- Incident Response with Splunk, Elastic SIEM

Module-10

Human Factors in Cyber Security

- Understanding Social Engineering: Identifying and mitigating human-centric threats.
- Insider Threats: Managing risks from within the organization.
- Developing Cybersecurity Awareness Programs: Strategies for effective training and awareness.
- Leadership in Cybersecurity: Building and managing high-performing cybersecurity teams.

Module-11

Industry-Specific Cybersecurity Challenges

- Cybersecurity in Financial Services: Protecting sensitive financial data and systems.
- Healthcare Cybersecurity: Safeguarding patient data and ensuring regulatory compliance.
- Cybersecurity in Critical Infrastructure: Securing essential services and national assets.
- Retail and E-commerce Cybersecurity: Addressing challenges in protecting consumer data.

Programme Modules

Module-12

Generative AI and Cybersecurity

- Introduction to Generative AI
- Increased risks and threats from Generative AI, innovation in cyber attacks
- Evolved threat identification through Generative AI
- Future of Generative AI and automation for containment and eradication

Module-13

Building and Managing a Cybersecurity Team

- Creating and leading a cybersecurity team
- Building and managing talent
- Evaluating performance
- Delegating responsibilities and tasks Addressing and resolving cultural issues

Module-14

Globalisation and Supply Chain Security

- Understanding supply chain cyber risks
- Causes of cybersecurity risks in supply chain
- Supply chain attacks
- Inadvertent threats in supply chain
- Malicious insider activity
- Role of leaders in supply chain cybersecurity
- Cybersecurity supply chain risk management
- Examples of supply chain cybersecurity responses

Module-15

Ethics Responsibilities and Future of Cybersecurity

- Legal and ethical responsibilities of cybersecurity leaders Evolving regulations and laws
- Building long-term cyber capabilities
- Emerging threats and technologies
- Ransomware case studies, critical infra protection case studies Insider threats
- Zero trust architecture
- Social engineering attacks

Capstone Project

In this three-part capstone project, learners will step into the role of a cybersecurity consultant. You will be tasked with designing a comprehensive, scalable, and future-proof cybersecurity framework tailored for a small-scale Indian business.

You'll begin by identifying key risks, designing a cybersecurity strategy, and ensuring regulatory compliance. As the business evolves, the framework will be enhanced by integrating advanced components such as AI, Business Continuity Planning, and Generative AI.

In the final phase, you'll future-proof the system by addressing emerging technologies, cloud security, supply chain risks, and team design. By the end of the project, you will have developed a real-world cybersecurity blueprint aligned with the needs of a dynamic organisation.

Over the duration of the programme, you will progressively build your project across three key phases:

Part A - Building the foundation
Part B - Evolving the strategy
Part C - Future-proofing the framework

Programme Faculty

Unlike traditional training, we embed industry veterans as faculty—bringing frontline experience from global cyber battles straight into our classrooms. Our unique model integrates practicing industry experts as faculty, ensuring learners gain battle-tested skills that go beyond textbooks and certifications.

Meet the Industry Change Makers

Founder & CEO BlackPerl
Ex-Amazon, Ex-Unilever
Over 15+ Years Industry Experience

Co-Founder & CTO BlackPerl
Cyber Architect over 16+ Years Industry Experience

Founder & CEO TerraEagle
Ex-CISO Unisys, Cyber Global Leader over 22+ Years Industry Experience

Programme Faculty

At GIM, leadership training is powered by master educators who combine academic rigor with real-world insights, creating an unmatched environment for leadership growth. Unlike conventional programs, GIM integrates globally acclaimed faculty whose proven mastery in leadership development ensures lasting impact on individuals and organizations.

Meet the Change Makers

Associate Professor
Member of IT Council of GCCI

Sr. Security Engineer - Blackperl DFIR
Over 5+ Years of Experience in the Industry

Associate Professor
Ph.D. from IDRBT

Programme Certificate

Upon successfully completing the programme with a minimum 70% score, you will be awarded a certificate from GIM & BlackPerl DFIR.

Who is this Programme For?

This programme is tailored to enhance your knowledge of essential principles and optimal methodologies in the field of cybersecurity. It will help you gain hands-on expertise in implementing cybersecurity measures for both immediate and future business strategies, and it will help you engage with consumer data and take responsibility for ensuring compliance with data privacy regulations.

Senior Leaders	Aspiring cybersecurity leaders	Students transitioning into Cyber Security	Professionals transitioning into Cyber Security
◦ Senior leaders who want to develop new applications and frameworks that will need to detect, withstand and counteract intrusion	◦ Aspiring cybersecurity leaders who want to lead security operations and new initiatives in their current organisation	◦ Students keen to gain cybersecurity skills and transition to a cybersecurity career	◦ Professionals keen to gain cybersecurity skills and transition to a cybersecurity career

Learning Journey

Orientation Week

Weekly Goals and Studies

Perform the Assessments and Tasks towards Projects

Final Certification Exam

About

Goa Institute of Management is a leading business school focused on transforming and improving management education.
Rated among the 'Best B-Schools for the World' in the Positive Impact Rating 2023, GIM endeavours to have a positive impact on the society through its 6 programs getting agile leaders ready for the world.

This year, **21%** PGDM Students received PPOs **55 L** Highest Package.

Goa Institute of Management is collaborating with BlackPerl DFIR Private Limited to to offer a portfolio of high-impact online programmes. BlackPerl is India’s Only Cyber Education Brand who has trained more than 16,000 students and industry professional in last one year with high quality, industry driven, job ready, practical oriented programmes. Working with BlackPerl gives GIM the advantage of broadening its access beyond their on-campus offerings in a collaborative and engaging format that stays true to the quality of GIM online programme.

Apply for the GIM's Advanced Cyber Security Programme for Leaders' here

Apply Now

Email: cybersecurityonline@gim.ac.in

Contact: +91-9960197556

In Collaboration with BlackPerl DFIR