According to *Forbes* in 2019, Cybersecurity is the number one business issue and Cyber events rank among the top three triggers for D&O derivative actions. The Marquette University Cybersecurity Certificate provides you with the latest strategies and tools to stay ahead of cyber events. Combining industry thought leaders and top instructors, you’ll develop the skills and knowledge to increase cyber resilience and face cyber challenges by elevating the experience and expertise of your firm.

An Outstanding Learning Experience

In 2001, 10% of business was digital; today, 85% of an organization’s value is digital. Everyone in the organization uses digital assets and must protect them. Now more than ever, companies must have effective cyber risk strategies. The Cybersecurity Certificate is a hands-on, four-day immersive experience where you learn to apply principles and techniques that drive cyber resiliency in the digital age. Roll up your sleeves and use live data in our laboratory to solve real-world challenges using the best practices developed by top companies. Our experts and professional instructors guide you through every step. The curriculum will help you build skills and create a unique roadmap enabling your company to thrive in the age of cybersecurity.

Instructors: Pioneers, Industry Leaders, Top Professionals and Experts

Gain access to our world-class faculty, including top academic researchers, leading practitioners and industry thought leaders. Our instructors and leadership work in, or consult with, the cybersecurity industry on a regular basis. Learn more about our program at marquette.edu/cyber-security-certificate.

The content of this certificate is based on the best-selling book *Managing Cyber Risk* by program creator and author Ariel Evans, and the VRisk platform, which enables students to have hands-on experiences.

JOIN OUR IN-CLASSROOM PROGRAM - $4,995

**SAMPLE SCHEDULE**

Each day includes breakfast and lunch. Please bring your own device (laptop or tablet) for online assignments. The program consists of 13 modules broken into 8 sessions, with the opportunity to choose your own track.

<table>
<thead>
<tr>
<th>Day</th>
<th>Time</th>
<th>Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day 1</td>
<td>9:00-12:00</td>
<td>The Evolution of Cybersecurity,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Basics, and Cyber Tools</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1:00-4:00 Cybersecurity Regulations</td>
</tr>
<tr>
<td>Day 2</td>
<td>9:00-12:00</td>
<td>GDPR and Privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1:00-4:00 NY DFS Part 500</td>
</tr>
<tr>
<td>Day 3</td>
<td>9:00-12:00</td>
<td>Cyber Insurance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1:00-4:00 Incident Response</td>
</tr>
<tr>
<td>Day 4</td>
<td>9:00-12:00</td>
<td>Risk Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1:00-4:00 Cybersecurity Strategy</td>
</tr>
</tbody>
</table>

APPLY TODAY: marquette.edu/cyber-security-certificate/
COURSE SUMMARY

The Marquette Cybersecurity Certificate is a rigorous four-day curriculum led by prominent cybersecurity experts, many of whom advise governments, agencies and industry bodies around the world. The course brings together executives, experts, innovators and regulators to address cybersecurity from a digital point of view. Away from your daily routine, you’ll be immersed in real-life challenges, expert thought leadership, hands-on applications, strategy sessions and innovation frameworks. Learn more at: marquette.edu/cyber-security-certificate/.

Based on three years of research with the Fortune 1000 and cyber insurance industry by Ariel Evans, the Marquette Cybersecurity Certificate Program consists of eight sessions that meet in the morning and afternoon. Below are the eight modules in the curriculum taught during the program. Each module is delivered in-person or online. The online application is open enrollment, offering maximum flexibility.

Before the class date, students are provided with access to the learning management system, prereading materials, textbook and course workbooks. A case study assignment with a template is provided to each student. Quizzes follow each module and are graded in class’ to facilitate students’ grasp of the concepts.

Module 1 Lesson 1: The Evolution of Cybersecurity
Learn about the evolution of cybersecurity from an IT issue into a business issue, business and technical roles, the consequences of poor cyber hygiene and trends.

• Introduction to Cybersecurity and Risk
• Digital Assets
• Cyber Consequences
• Cyber Trends and Spending
• Cyber Roles and Responsibilities

Module 1 Lesson 2: Cybersecurity Basics
Learn to communicate and speak the language of cyber. Understand how attacks happen and why. Learn to speak about data breaches intelligently. Includes data breach case studies.

• Attack Surfaces
• Terminology
• Enterprise Threats of Today
• Enterprise Cybersecurity Programs
• Data Breach Case Studies

Module 1 Lesson 3: Cyber Tools
Understand what a cybersecurity tool is and understand various cyber tools based on organizational maturity

• NIST Functional Correlation
• Tool Maturity
• Cyber Policies
• Tool Purposes and Usage

Module 2: Cybersecurity Regulations
Take a deep dive into cybersecurity regulations across geographies, governments, data types and industries

• U.S. Government
• State Regulation
• Industry Regulation
• Privacy, Credit Card and Health Care Regulation

APPLY TODAY: marquette.edu/cyber-security-certificate/
Module 3: GDPR
Learn about the requirements of the General Data Protection Regulation as it applies to the use and collection of privacy data and system security requirements.

- Scope of the GDPR
- GDPR Articles – What Do They Mean
- Preparation, Enforcement and Penalties
- Developing a GDPR Program
- Organizational Requirements
- System Requirements
- Privacy Impact Assessment

Module 4: NY DFS 500
Learn about the New York State Department of Financial Services Cybersecurity Law for Financial Institutions.

- Scope
- History
- Requirements

Module 5: Cyber Insurance
Learn how to quantify cyber insurance, first vs. third party risk, gaps in current D&O policies and how cyber claims get paid.

- Types of Cyber Insurance
- Cyber Insurance Quantification
- Trends and Statistics
- Insurance Quantification

Module 6: Incident Response
Learn about investigation goals, evidence collection techniques and planning. Discusses cyber response planning, data collection and processing with acceptable law enforcement standards.

- Cyber Response Plan
- Prevention of Criminal Activity
- Forensic Techniques and Monitoring Practices
- Table-top Exercise

Module 7: Risk Management
Learn how to quantify and score cyber risk.

- Inherent Risk Scoring
- Residual Risk Scoring
- Risk Exposure Quantification
- Risk Assessments
- Third Party Cyber Risk
- Cyber Risk Management

Module 8: Cybersecurity Strategy
Translate cyber risk management metrics into an effective and resilient security strategy for an organization.

- Strategic Terms and Relationships
- Cyber Thresholds
- Cyber Tool ROI
- Vendor Risk
- Budgeting and Prioritizing
- M&A
DISTINGUISH YOURSELF AS A LEADER WITH YOUR CYBERSECURITY CERTIFICATE

The Marquette University Certificate provides you the knowledge and differentiating factor. It proves that you have completed all modules as well as the cumulative Capstone Project. You walk away with confidence and your professional Cybersecurity Portfolio.

Learn more at: marquette.edu/cyber-security-certificate/