MassMutual – Cyber Security

University of Massachusetts - Internship Opportunities Within Enterprise Information Risk Management

- Information Risk Policies and Standards
- Cyber Intelligence / Security Operations
- Access Management
- Security Controls Management
- Incident Response
- Threat Intelligence
- Digital Forensics and Investigations
- Security Architecture / Engineering / Tools
- Information Risk
- Third Party Risk Management
- Security Awareness, Training & Communication
Position Information

Position Title: Security Engineering Intern
Job Location: Springfield, MA
Business Unit: IT Operations
Department Name: Enterprise Resilience & Information Protection Services
Schedule for Intern: Full-time, 40 hours/wk, 9 weeks

Department Overview:
Enterprise Resilience & Information Protection Services is responsible for ensuring the operating stability of MassMutual, governing how information is stored and destroyed, and deploying world-class capabilities in the area of cyber security.

Position Description:
We are a major Fortune 500 insurance and financial services company with a razor-sharp focus on protecting the company's information assets. MassMutual has implemented a strong information risk program and we are looking to expand its capabilities with a world class Information Protection Services. Ultimately, we want to proactively protect MassMutual's digital assets through a combination of security engineering expertise and industry leading tools.

The Security Engineering intern will work with state of the art tools and seasoned IT Engineers to detect and mitigate vulnerabilities in MassMutual's operating environment.

If you are interested in getting us started down this new path, read on...

What we can do for you
We can offer you the ability to show your stuff and build your skills, by working on projects that will transform the way we approach information risk management.

You will learn how prompt detection, containment, and eradication of sophisticated cyber threats can have practical and game-changing impacts on real businesses – and how to frame your skills in a way that is attractive to employers in many industries.

You’ll do this by:
- Designing and implementing creative approaches to detect & prevent cyber crime
- Leveraging your technical skills to analyze & respond to information security incidents
- Building your real-world security knowledge in implementing and maintaining enterprise network / infrastructure security products & tools
- Influencing our security operations strategy through research and competitive analysis

Daily Tasks & Responsibilities:

- Gathering and reporting metrics
- Learning and using Archer our GRC platform
- Learning and using Qualys our environmental scanning tool
- Partnering with security engineers to develop remediation plans that are technology specific
- Other duties as assigned

Top 3 Skills and Abilities Needed to Succeed:

1. Task-oriented: Assign owners, agree to dates, drive to completion
2. Influencing: Help people understand the importance of this work effort
3. Communication: Written and verbal
POSITION INFORMATION

Position Title: Information Security Intern
Job Location: Springfield, MA
Business Unit: Enterprise Information Risk Management (EIRM)
Department Name: Security Controls Management
Schedule for Intern: Full-time, 40 hours/wk, 9 weeks

DEPARTMENT OVERVIEW:

Enterprise Information Risk Management (EIRM) is responsible for securing the digital assets of the firm.

POSITION DESCRIPTION:

We are a major Fortune 500 insurance and financial services company with a razor-sharp focus on protecting the company’s information assets. MassMutual has implemented a strong information risk program and we are looking to expand its capabilities with a world class Security Controls Management program. Ultimately, we want to proactively protect MassMutual’s digital assets through a continuous improvement process of designing and testing the controls that protect our digital assets.

The Security Controls intern will work with the Information Rick Assurance team to address security controls design and assessment in collaboration with our lines of business areas to enhance the security effectiveness of our controls.

If you are interested in working with a cutting edge team and learning how we protect the digital assets of the firm...Read on!

What we can do for you
We can build out your risk and security “Mindset” in line with your educational and career goals, while providing practical hands on information risk experience to boost that resume.

You will learn how well designed controls contribute to the overall proactive detection, containment, and eradication of sophisticated cyber threats targeting our information assets. The appropriate controls maintain a level of protection providing a sense of security and protection for the brand of the firm and customer confidence.

You’ll do this by:
• Designing and implementing creative to apply controls to our information assets
• Leveraging your technical skills to understand gaps in security and how to plug the holes
• Building your real-world security & controls knowledge in implementing and maintaining an enterprise information controls procedure framework.
• Influencing our security controls strategy through research and competitive analysis – maintaining currency with leading polices standards and controls

DAILY TASKS & RESPONSIBILITIES:

• Assist with performing control gap assessments and analysis
• Maintain key risk indicators and metrics of control effectiveness
• Collaborate with security teams to define and design effective control solutions

TOP 3 SKILLS AND ABILITIES NEEDED TO SUCCEED:

1. Good understanding of computer systems – primarily Windows
2. Good communication skills & Business Acumen
3. Basic understanding of how to use Microsoft Office products
**POSITION INFORMATION**

<table>
<thead>
<tr>
<th>Position Title:</th>
<th>Information Security Intern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Location:</td>
<td>Springfield, MA</td>
</tr>
<tr>
<td>Business Unit:</td>
<td>Enterprise Information Risk Management (EIRM)</td>
</tr>
<tr>
<td>Department Name:</td>
<td>Cyber Intelligence / Security Operations</td>
</tr>
<tr>
<td>Schedule for Intern:</td>
<td>Full-time, 40 hours/wk, 9 weeks</td>
</tr>
</tbody>
</table>

**DEPARTMENT OVERVIEW:**

Enterprise Information Risk Management (EIRM) is responsible for securing the digital assets of the firm.

**POSITION DESCRIPTION:**

We are a major Fortune 500 insurance and financial services company with a razor-sharp focus on protecting the company’s information assets. MassMutual has implemented a strong information risk program and we are looking to expand its capabilities with a world class security operations center. Ultimately, we want to proactively protect MassMutual’s digital assets through a combination of threat intelligence, vulnerability management and incident response.

The Security Operations Center (SOC) intern will work with the SOC team to address security alerts generated by our monitoring systems.

If you are interested in getting us started down this new path, read on...

**What we can do for you**

We can offer you the ability to show your stuff and build your skills, by working on projects that will transform the way we approach information risk management.

You will learn how prompt detection, containment, and eradication of sophisticated cyber threats can have practical and game-changing impacts on real businesses – and how to frame your skills in a way that is attractive to employers in many industries.

**You’ll do this by:**

- Designing and implementing creative approaches to detect & prevent cyber crime
- Leveraging your technical skills to analyze & respond to information security incidents
- Building your real-world security knowledge in implementing and maintaining enterprise network / infrastructure security products & tools
- Influencing our security operations strategy through research and competitive analysis

**DAILY TASKS & RESPONSIBILITIES:**

- Review security alerts and follow documented response processes
- Maintain status information on alerts to ensure the events are being addressed appropriately
- Provide information on daily activities for the Security Operations and Threat Intelligence morning huddle

**TOP 3 SKILLS AND ABILITIES NEEDED TO SUCCEED:**

1. Good understanding of computer systems – primarily Windows
2. Good communication skills
3. Basic understanding of how to use Microsoft Office products
POSITION INFORMATION

<table>
<thead>
<tr>
<th>Position Title:</th>
<th>Information Security Intern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Location:</td>
<td>Springfield, MA</td>
</tr>
<tr>
<td>Business Unit:</td>
<td>Enterprise Information Risk Management (EIRM)</td>
</tr>
<tr>
<td>Department Name:</td>
<td>Security Awareness, Training &amp; Communication</td>
</tr>
<tr>
<td>Schedule for Intern:</td>
<td>Full-time, 40 hours/wk, 9 weeks</td>
</tr>
</tbody>
</table>

DEPARTMENT OVERVIEW:

Enterprise Information Risk Management (EIRM) is responsible for securing the digital assets of the firm.

POSITION DESCRIPTION:

We are a major Fortune 500 insurance and financial services company with a razor-sharp focus on protecting the company’s information assets. MassMutual has implemented a strong information risk program and we are looking to expand our capabilities with a world class Security Awareness, Training and Communication Program. Ultimately, we want to proactively protect MassMutual’s digital assets through increasing employee, customer and subsidiary awareness and understanding of what behaviors can best protect MassMutual from the bad guys.

The Security Awareness, Training & Communications intern will work with our Security Awareness Team to educate associates across the company about how to make MassMutual a cyber resilient organization.

If you are interested in getting us started down this new path, read on...

**What we can do for you**

We can offer you the ability to show your stuff and build your skills, by working on projects that will transform the way we approach information risk management. You’ll learn how Information Risk Awareness can have practical and game-changing impacts on real businesses – and how to frame your skills in a way that is attractive to employers in many industries.

**You’ll do this by:**

- Marketing and communicating unique messages focused on securing MassMutual’s information assets.
- Leveraging entrepreneurial drive to discover novel opportunities for educating employees across MassMutual.
- Building your communication skills through the development and delivery of key Information Risk messages.
- Working hard with a passion for meeting and influencing our employee base.

DAILY TASKS & RESPONSIBILITIES:

- Writing and delivering content to key roles across the organization.
- Planning and participating in a variety of cyber resiliency events that take place throughout the year.
- Supporting the marketing and communication of a number of security initiatives.

TOP 3 SKILLS AND ABILITIES NEEDED TO SUCCEED:

- Written and verbal communication
- Customer Service
- Creativity
POSITION INFORMATION

Position Title: Information Security Intern
Job Location: Springfield, MA
Business Unit: Enterprise Information Risk Management (EIRM)
Department Name: Information Risk Policies and Standards
Schedule for Intern: Full-time, 40 hours/wk, 9 weeks

DEPARTMENT OVERVIEW:

Enterprise Information Risk Management (EIRM) is responsible for securing the digital assets of the firm.

POSITION DESCRIPTION:

We are a major Fortune 500 insurance and financial services company with a razor-sharp focus on protecting the company’s information assets. MassMutual Information Risk Policies and Standards Framework is the focal point for managing risks associated with MassMutual’s information technology resources and for protecting MassMutual’s information assets. These policies and standards set a baseline in accordance with industry best practice and provide the business with a platform to protect information assets, commensurate with business risk.

The Information Risk Policies and Standards intern will work with our Policies and Standards Team to ensure our framework is positioning MassMutual to proactively address emerging regulatory and technology trends.

If you are interested in getting us started down this new path, read on...

What we can do for you
We can offer you the ability to show your stuff and build your skills, by working on projects that will transform the way we approach information risk management. You’ll learn how Information Risk Policies and Standards can have practical and game-changing impacts on real businesses – and how to frame your skills in a way that is attractive to employers in many industries.

You’ll do this by:
• Researching emerging regulatory trends for potential impacts to MassMutual.
• Researching emerging technology trends (wearables, mobility, cloud) for potential impacts to MassMutual.
• Supporting efforts to address non-conformance to policies and standards.
• Working hard with a passion for influencing key MassMutual initiatives.

DAILY TASKS & RESPONSIBILITIES:

• Researching a variety of emerging trends for potential disruptors or enablers for MassMutual.
• Planning and participating in a variety of cyber resiliency initiatives that take place throughout the year.
• Supporting a variety of team initiatives.

TOP 3 SKILLS AND ABILITIES NEEDED TO SUCCEED:

• Written and verbal communication
• Customer Service
• Research and Analysis
POSITION INFORMATION

<table>
<thead>
<tr>
<th>Position Title:</th>
<th>Information Risk Intern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Location:</td>
<td>Springfield, MA</td>
</tr>
<tr>
<td>Business Unit:</td>
<td>Enterprise Information Risk Management (EIRM)</td>
</tr>
<tr>
<td>Department Name:</td>
<td>Information Risk Management</td>
</tr>
<tr>
<td>Schedule for Intern:</td>
<td>Full-time, 40 hours/wk, 9 weeks</td>
</tr>
</tbody>
</table>

DEPARTMENT OVERVIEW:

Enterprise Information Risk Management (EIRM) is responsible for securing the digital assets of the firm.

POSITION DESCRIPTION:

We are a major Fortune 500 insurance and financial services company with a razor-sharp focus on protecting the company’s information assets. MassMutual has implemented a strong information risk management program and effective information risk management is central to our program. Information Risk Management is the disciple of identifying, analyzing, and communicating the information risk to the business area.

The Information Risk Management (IRM) intern will work with the IRM team to identify risk that could impact our business areas.

If you are interested in getting us started down this new path, read on...

**What we can do for you**

We can offer you the ability to show your stuff and build your skills, by working on projects that will transform the way we approach information risk management.

You will learn how assess risk, conduct due diligence reviews, communications findings to the business area, and how the development of compensating controls can help reduce the risk to the business.

**You’ll do this by:**

- Leveraging your technical skills to analyze & respond to information risks
- Building your real-world information risk management knowledge by identifying risk, conducting analysis and communicating the impacts to the business areas
- Influencing our information risk management strategy through research and competitive analysis

DAILY TASKS & RESPONSIBILITIES:

- Review daily metrics for potential indicators of risk and follow documented tracking processes
- Reconcile daily reports to identify high risk items to ensure the risks are being mitigated appropriately
- Partner with experienced IRMs to assess risk, design compensating controls, and communicate findings to the appropriate business area

TOP 3 SKILLS AND ABILITIES NEEDED TO SUCCEED:

1. Good communication skills
2. Good understanding of computer systems – primarily Windows
3. Basic understanding of how to use Microsoft Office products
POSITION INFORMATION

Position Title: Information Risk Intern
Job Location: Springfield, MA
Business Unit: Enterprise Information Risk Management (EIRM)
Department Name: Information Risk Management
Schedule for Intern: Full-time, 40 hours/wk, 9 weeks

DEPARTMENT OVERVIEW:

Enterprise Information Risk Management (EIRM) is responsible for securing the digital assets of the firm.

POSITION DESCRIPTION:

We are a major Fortune 500 insurance and financial services company with a razor-sharp focus on protecting the company's information assets. MassMutual has implemented a strong information risk management program and the effective risk management of 3rd Party Suppliers is critical to our success. 3rd Party Supplier Risk Management is the discipline of identifying, analyzing, and communicating the information risk of our 3rd Party Suppliers.

The 3rd Party Supplier Risk Management intern will work with the 3rd Part Supplier team to identify risk that could impact our business areas.

If you are interested in getting us started down this new path, read on...

What we can do for you
We can offer you the ability to show your stuff and build your skills, by working on projects that will transform the way we approach information risk management.

You will learn how assess risk, conduct due diligence reviews, communications findings to the business area, and how the development of compensating controls can help reduce the risk to the business.

You’ll do this by:
• Leveraging your technical skills to analyze & respond to information risks
• Building your real-world supplier risk management knowledge by identifying risk, conducting analysis and communicating the impacts to the business areas
• Influencing our supplier information risk management strategy through research and competitive analysis

DAILY TASKS & RESPONSIBILITIES:

• Review daily metrics for potential indicators of risk and follow documented tracking processes
• Reconcile daily reports to identify high risk items to ensure the risks are being mitigated appropriately
• Partner with experienced associates to assess risk, design compensating controls, and communicate findings to the appropriate business area and the 3rd Party Supplier

TOP 3 SKILLS AND ABILITIES NEEDED TO SUCCEED:

1. Good communication skills
2. Good understanding of computer systems – primarily Windows
3. Basic understanding of how to use Microsoft Office products
**POSITION INFORMATION**

Position Title: Information Security Intern  
Job Location: Springfield, MA  
Business Unit: Enterprise Information Risk Management (EIRM)  
Department Name: Cyber Incident Response  
Schedule for Intern: Full-time, 40 hours/wk, 9 weeks

**DEPARTMENT OVERVIEW:**

We protect MassMutual’s brand through the facilitation of containment, eradication, and remediation of cyber incidents.

**POSITION DESCRIPTION:**

The Cyber Incident Response intern will work with key stakeholders from across the enterprise (IT operations, legal, compliance, enterprise risk management, PR, etc.) to prepare the organization to respond swiftly to cyber incidents.

If you are interested in getting us started down this new path, read on...

**What we can do for you**

We can offer you the ability to show your stuff and build your skills, by working on projects that will transform the way we approach cyber incident response.

You will learn about the value of professional relationships through the use of our matrix organization to resolve cyber incidents – and how to frame your skills in a way that is attractive to employers in many industries.

**You’ll do this by:**

• Developing, testing, and updating incident response playbooks  
• Facilitate testing exercises with key stakeholders  
• Participate in process flow mapping sessions  
• Develop simple and meaningful metrics to measure and improve incident response capabilities

**DAILY TASKS & RESPONSIBILITIES:**

• Follow up on remediation steps and process improvement updates  
• Documentation updates  
• Participate in any current incidents

**TOP 3 SKILLS AND ABILITIES NEEDED TO SUCCEED:**

1. Good communication & facilitation skills  
2. Problem solving and planning skills  
3. Basic understanding of how to use Microsoft Office products
POSITION INFORMATION

Position Title: Threat Intelligence Intern
Job Location: Boston, MA
Business Unit: Enterprise Information Risk Management (EIRM)
Department Name: Cyber Threat Intelligence
Schedule for Intern: Full-time, 40 hours/wk, 9 weeks

POSITION DESCRIPTION:

We are a major Fortune 500 insurance and financial services company with a strong focus on protecting the company’s digital assets. MassMutual has implemented a comprehensive information security program and we are looking to expand its capabilities through a world-class cyber intelligence unit. Ultimately, we want to proactively defend MassMutual’s network, endpoints, and employees through a combination of threat intelligence, vulnerability management, ethical hacking, security operations and incident response.

If you are interested in getting us started down this new path, read on...

What we can do for you
We can offer you the ability to show your stuff and build your skills, by working on projects that will transform the way we approach information risk management.

You will learn how prompt detection, containment, and eradication of sophisticated cyber threats can have practical and game-changing impacts on real businesses – and how to frame your skills in a way that is attractive to employers in many industries.

You’ll also gain the following skills:
• Basic understanding of Advanced Persistent Threats (APTs), cyber criminals, hacktivists and their associated tactics, techniques, and procedures (TTPs).
• Ability to participate in the analysis of threat intelligence materials, vulnerability reports, malware samples, and network security events for purposes of defining and providing early indicator and warning (I&W) of cyber threats targeting MassMutual’s network.
• Ability to maintain, develop, and continually evaluate threat intelligence sources (technical & non-technical) to increase effectiveness and timeliness of reporting to senior analysts.

Scope:
The intern will focus on providing intelligence analysis support as part of a team that is performing in-depth technical analysis of advanced cyber threats by utilizing innovative technologies to determine adversarial intent and capabilities.

REQUIRED SKILLS:

• Demonstrated ability to research, analyze, and synthesize large amounts of data and information (internal attacks, portal and open source threat intelligence data) to correlate current and emerging threat trends.
• Strong problem solving and critical thinking capabilities are essential to assisting a fast-paced, analytical team.
• Clear writing, communications, and presentation skills are critical.

TOP 3 SKILLS AND ABILITIES NEEDED TO SUCCEED:

1. Ability to read and understand network log sources and events (netflow, packet capture)
2. Basic knowledge of programming languages (Python) to work with structured and unstructured threat data
3. Experience utilizing data visualization platforms (Maltego) to map out threat infrastructure.