How to Reduce Cyber Insurance Premiums:

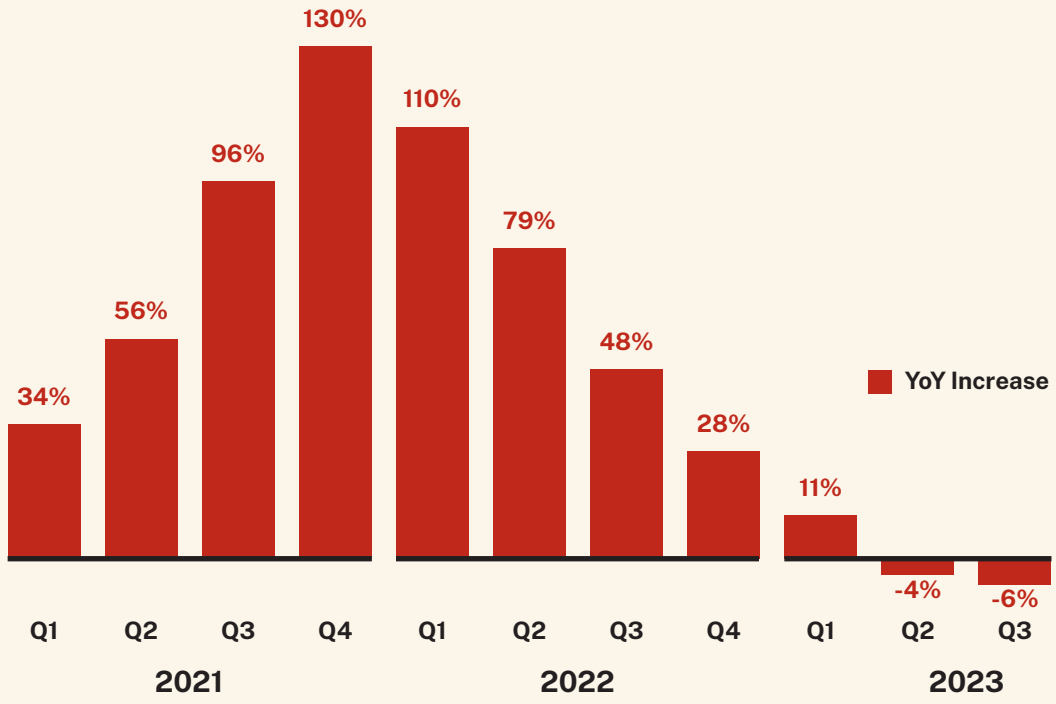
3 Actionable Checklists

Balbix®

Introduction:

Navigating the Cyber Insurance Maze

The astronomical cost of cyber insurance has surged in recent years, reflecting the escalating frequency and severity of cyberattacks. As companies rely more on diverse digital platforms and cloud services, often with scattered security oversight, the financial implications of data breaches, ransomware attacks, and other cyber incidents have grown. In Dark Reading's January 2024 report "*With Attacks on the Upswing, Cyber-Insurance Premiums Poised to Rise Too*," it states that despite a lull in premium increases in 2023, cyber insurance premiums are poised to continue their dramatic rise, which began in 2021.



Cyber Security Rate Increases 2021-2023

This rise in risk exposure and the opportunity for breach mitigation costs and compliance fines (especially with new regulations and disclosure requirements by global regulators i.e. SEC, NIS2, DORA, etc.) is leading insurers to hike premiums, impose stricter coverage requirements, and in some cases, reduce the limits on policies.

The good news is that premiums can be substantially reduced even in this increasingly risky environment. In this guide, we explore the multifaceted art of managing cyber risks to protect digital assets and prevent cyber insurance premiums from undermining your budget. We devised a structured three-step approach that harmonizes the reduction of potential risks, the fostering of continuous improvement in cyber resilience, and strategic interactions with insurance providers to effectively drive down costs.

STEP 1:

Mitigate Cyber Risks Contributing to Skyrocketing Insurance

To navigate the complexities of cyber insurance effectively, it is crucial to understand and mitigate the five risks that most significantly elevate insurance costs. These originate from two main sources: human errors and technological flaws.

Caused by Human Error

1. **Ransomware Attacks**: Although ransomware exploits technological vulnerabilities, such as security gaps in software or systems, it often relies on human oversight such as, clicking malicious links or opening infected email attachments to initiate the attack.
2. **Data Breaches:** These can occur through both technology flaws and human error, but a significant number of data breaches are the result of human actions such as falling for phishing scams, poor security practices like weak passwords, or mishandling data.
3. **Business Email Compromise (BEC):** BEC attacks are almost entirely predicated on social engineering techniques that manipulate individuals into making wire transfers or divulging sensitive information. They exploit human psychology rather than technological weaknesses.

Caused by Technology Flaws

4. **Cloud Vulnerabilities:** These often stem from misconfigurations or flaws in the security architecture of cloud services. While human error can contribute to misconfigurations, the complexity and inherent vulnerabilities within the technology itself play a significant role.
5. **Supply Chain Attacks:** These attacks exploit vulnerabilities in software or hardware that stem from third-party suppliers. The technology flaws may be in the software development or update distribution processes, which are then exploited to compromise the target organization.

Risk Remediation Checklist

The following checklist contains milestones that must be reached to fulfill each of the risk remediation requirements demanded by cyber insurers.

Ransomware Mitigation Steps

- [ ] **Robust Backup and Recovery:** Implement and regularly test backup solutions to ensure data can be restored quickly without paying a ransom.
- [ ] **Security Awareness Training:** Educate employees on recognizing phishing and spear-phishing attempts to prevent the successful delivery of ransomware.
- [ ] **Patch Management:** Regularly update and patch systems, software, and applications to close off vulnerabilities that could be exploited by ransomware.
- [ ] **Endpoint Protection:** Use advanced antivirus and anti-malware solutions with ransomware detection capabilities.

Data Breach Mitigation Steps

- [ ] **Data Encryption:** Encrypt sensitive data both in transit and at rest to protect it even if unauthorized access occurs.
- [ ] **Access Controls:** Implement strict access controls and use the principle of least privilege to limit access to sensitive data.
- [ ] **Regular Audits:** Conduct regular security audits and vulnerability assessments to identify and mitigate risks.
- [ ] **Incident Response Plan:** Develop and routinely test an incident response plan to reduce the impact of a data breach.

Business Email Compromise (BEC) Mitigation Steps

- [ ] **Email Filtering:** Use advanced email security solutions that can detect and block fraudulent emails.
- [ ] **User Verification Protocols:** Establish protocols to verify the authenticity of requests for fund transfers or confidential information, especially those that are urgent or change previously established payment details.
- [ ] **Training and Awareness:** Continuously educate employees about BEC schemes and encourage them to double-check email addresses and other identifiers for authenticity.

Vulnerability Mitigation Steps

- [ ] **Prioritize and Remediate Risks:** Prioritize risks for remediation based on the potential financial impact a breach would have on the organization.
- [ ] **Cloud Security Posture Management (CSPM):** Deploy CSPM tools to identify and remediate misconfigurations and compliance violations in cloud environments.
- [ ] **Strong Authentication and Access Controls:** Use multi-factor authentication and enforce strong access controls for cloud resources.
- [ ] **Regular Security Assessments:** Periodically review and audit security settings and practice**s.**

Supply Chain Attack Mitigation Steps

- [ ] **Vendor Risk Management:** Conduct thorough security assessments of all vendors and third-party service providers. Continuously monitor and manage the security postures of all partners.
- [ ] **Segmentation and Isolation:** Use network segmentation to isolate critical systems and data from third-party access.
- [ ] **Continuous Monitoring:** Implement tools to continuously monitor for unusual activities that could indicate a compromise through the supply chain.

STEP 2:

Implement Continuous Cyber Posture Improvement

Implementing Continuous Threat Exposure Management (CTEM) is essential for showing insurers that you are maintaining a proactive stance against cyber threats. In addition, Gartner identified Continuous Threat Exposure Management (CTEM) as one of the top 10 technology trends.

CTEM enhances your security by continuously scanning for vulnerabilities, allowing for prompt and effective prioritization and resolution. This not only reduces the likelihood of successful attacks but also demonstrates to insurers a commitment to maintaining optimal security standards. By documenting and regularly updating security practices and compliance, CTEM also supports favorable assessments during insurance evaluations. This approach keeps you ahead of threats by:

- **Identifying and Prioritizing:** Continuously scanning the horizon for vulnerabilities and intelligently prioritizing them ensures you tackle the most impactful issues first.
- **Reducing Response Times:** When incidents occur, the speed of your response can mean the difference between a footnote and a front-page scandal.
- **Showcasing Security Maturity:** Regularly updated metrics and compliance with industry standards not only bolster your defenses but also shine during insurance evaluations.

CTEM Program Implementation Checklist

The following is a checklist for fulfilling the requirements for the CTEM 5-step program.

- [ ] **Vulnerability Prioritization Strategy:** Expanded focus from zero-day vulnerabilities to include those with a more direct impact, prioritizing based on severity, asset criticality, and business impact.
- [ ] **Team Capacity & Workflow Efficiency:** Automation has alleviated the burden on IT and security teams, enhancing productivity and reducing manual workload.
- [ ] **Reporting & Metrics:** Refined reporting highlights improvements in security posture and provides quantifiable risk reduction metrics to stakeholders.
- [ ] **Integration & Automation:** A unified vulnerability management system now integrates and automates continuous monitoring across our IT landscape.
- [ ] **Strategic Alignment:** Vulnerability management strategy is now tightly aligned with both cybersecurity and business objectives, adapting to evolving threats and needs.
- [ ] **Stakeholder Communication:** Have bridged the communication gap between technical teams and non-technical stakeholders, ensuring clarity and comprehension of cybersecurity metrics.
- [ ] **Continuous Improvement:** Foster continuous improvement, regularly updating our processes to stay abreast of new threats and technological advancements.
- [ ] **Risk Management Integration:** Vulnerability management is fully integrated within our broader risk management framework, enabling effective prioritization of actions based on financial risk assessments.

STEP 3:

Master the Insurance Negotiation Game

Prepare to negotiate with current or potential cyber insurance providers with these four steps:

Review your cybersecurity measures and document any improvements and their impact.

Show how your cybersecurity efforts reduce the financial risks.

Get third-party validations for your security measures.

Use this information to approach different insurers for the best coverage and premium options.

Once you've done these, you're ready to negotiate with insurance providers to secure the best coverage options and premiums. We included a detailed list below of the top ten things to consider when negotiating with cyber insurance providers.

Insurance Negotiation Checklist

Before scheduling a meeting with cyber insurance providers to negotiate policy premiums and terms, you should make sure that each of the following are addressed and documented in a way that you can present them during your meeting.

- [ ] **Assess Current Cybersecurity Posture**: Before approaching insurers, CISO should thoroughly review the organization's current cybersecurity measures, vulnerabilities, and risk levels. This includes understanding the scope of coverage needed based on potential risks and previous security incidents.

- [ ] **Implement Robust Security Measures**: Ensure that the organization adheres to best practices in cybersecurity, including deploying advanced security technologies, maintaining up-to-date systems and software, implementing strict access controls, and continuously monitoring the security environment. Adopting frameworks like CTEM can also show a proactive approach to managing and mitigating risks.

- [ ] **Document Security Improvements and Outcomes**: Keep detailed records of all cybersecurity improvements and their impacts. This should include changes made to the security infrastructure, training programs conducted, incidents handled, and how quickly and effectively they were resolved. Documentation should also highlight the continuous improvement in security metrics over time.

- [ ] **Quantify Risk Reduction**: Use tools to quantify the financial impact of potential risks and demonstrate how your cybersecurity measures have reduced this exposure. Cyber Risk Quantification (CRQ) can effectively translate technical risks into financial terms that insurers can easily understand and evaluate.

- [ ] **Gather Third-Party Assessments**: Obtain assessments from independent auditors or security firms that validate the effectiveness of your cybersecurity practices. This third-party validation can add credibility to your security posture claims.

- [ ] **Prepare a Presentation for Insurers**: Develop a comprehensive presentation that includes all the above details. The presentation should clearly outline how your cybersecurity practices not only comply with industry standards but also reduce the risk of significant financial loss from cyber incidents.

- [ ] **Engage with Multiple Insurers**: Don't limit your options to one insurance provider. You can compare coverage options and premium offers by engaging with multiple insurers. This also gives you negotiation leverage, as insurers will know they are competing for your business.

- [ ] **Highlight Compliance with Regulations**: Demonstrate compliance with all relevant regulations and standards. This shows insurers that your organization is less likely to face regulatory penalties or damages from non-compliance, which can influence premium calculations.

- [ ] **Discuss Long-Term Partnerships**: Show your commitment to maintaining and improving your cybersecurity measures over time. Insurers are more likely to offer better rates if they see that an organization is committed to long-term security and risk management.

- [ ] **Negotiate Terms Based on Demonstrated Risk Management**: Use the documented improvements and third-party validations to negotiate terms. Highlight how your proactive risk management strategies, like CTEM, reduce the insurer's risk and justify lower premiums.

How Balbix Can Help

It all boils down to speaking the language of insurance underwriters: Money. More specifically, money that you save your company and money that the insurance company will not need to pay out in the event of a breach.

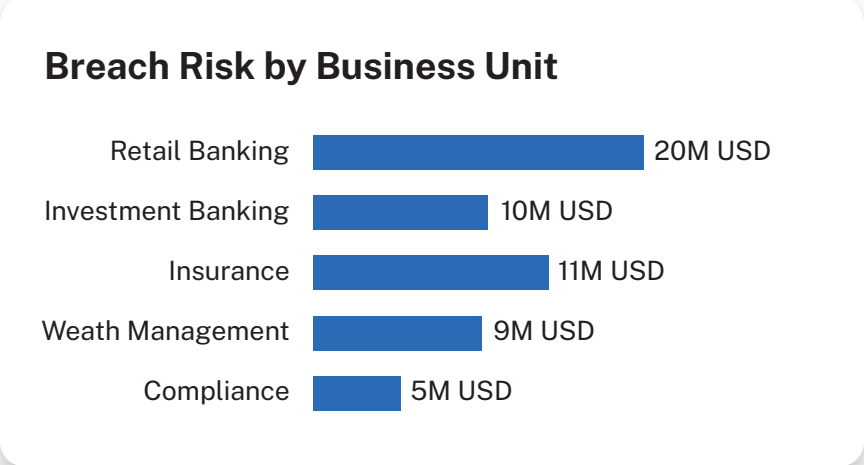
Many CISOs mistakenly believe that presenting risks and remediation strategies in technical terms to insurers demonstrates a strong cyber posture justifying more affordable insurance rates. Unfortunately, insurers, like boards, are not technical experts, and overly detailed reports about breaches stopped and vulnerabilities mitigated often cause eyes to glaze over.

From a functionality standpoint, underwriters are looking for five types of security enhancements, although these need to be translated into terms of financial savings:

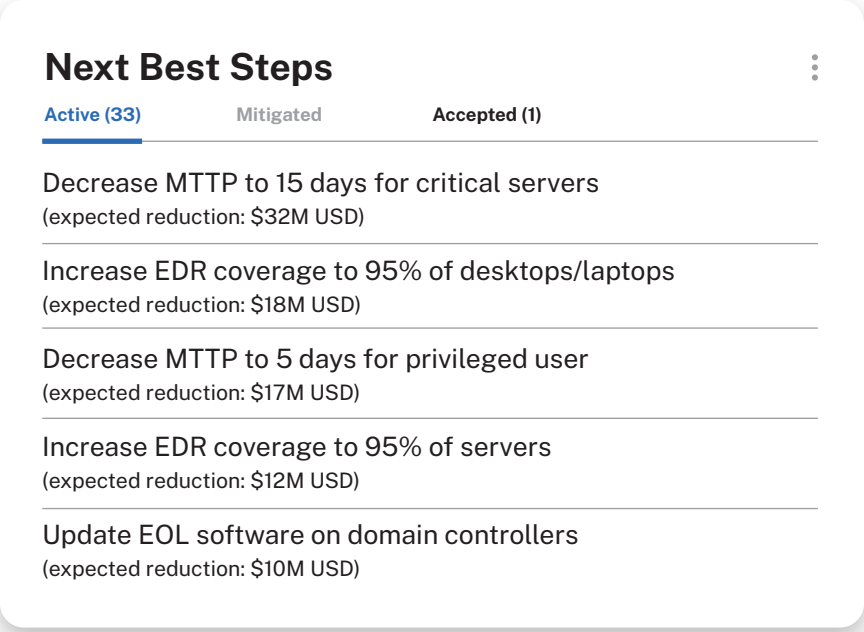
	What underwriters look for...	What Balbix delivers...
1	**Effective Risk Assessment and Mitigation:** Underwritten organizations should conduct regular and comprehensive risk assessments to identify vulnerabilities in their environment. Additionally, they must demonstrate robust risk mitigation strategies to address these vulnerabilities. Insurers often reward proactive risk management efforts with lower premiums.	**Prioritize High-Impact Risks for Remediation:** Balbix enables you to target and mitigate risks with the most significant financial impact to your organization. By prioritizing vulnerabilities based on their financial impact, you can direct resources where they'll make the most significant difference and communicate potential savings while reducing risk. Balbix also enables quick burn down of cyber risk with prioritized patching, automated workflows, and gamification.
2	**Vendor Risk Management:** Underwritten organizations should assess and manage the cybersecurity risks posed by third-party vendors and service providers. Insurers often consider the security practices of your vendors when calculating premiums, so ensuring that they meet stringent cybersecurity standards can positively impact your insurance costs.	**Application Inventory & Risk Management:** Balbix enables security teams to overcome asset visibility and exposure challenges by providing organizations with a near real-time, up-to-date comprehensive and unified view of your assets and software, including IaaS and PaaS, as well as their vulnerabilities, clearly mapping your attack surface.
3	**Continuous Monitoring and Auditing:** Underwritten organizations must implement continuous monitoring tools and conduct regular cybersecurity audits to detect and address security gaps promptly. Demonstrating a proactive approach to cybersecurity monitoring and compliance can lower insurance premiums.	**Track and Improve Maturity Against NIST:** Balbix helps you continuously analyze data from your tools and track the effectiveness of your security program's Identify, Protect, Detect, Respond, Recover and Govern (with the release of NIST CSF v2.0) functions in a data-driven manner. Actionable insights surfaced by Balbix help you close your gaps and improve your risk scores.
4	**Incident Response Planning:** Underwritten organizations should develop and regularly update an incident response plan to ensure swift and effective responses to cyber incidents. Having a well-defined plan can minimize the impact of breaches and demonstrate to insurers that you're prepared to handle cyber threats, potentially leading to lower premiums.	**Incident Analysis and Prevention:** Balbix can provide critical context for incident responders with respect to assets and applications, particularly with respect to materiality of the asset.
5	**Compliance with Regulatory Standards:** Underwritten organizations should ensure compliance with relevant cybersecurity regulations and industry standards. Meeting regulatory requirements not only helps protect your organization from fines and legal penalties but also demonstrates to insurers that you take cybersecurity seriously, potentially leading to premium discounts.	**Faster Audit & Compliance:** Balbix helps you meet service level agreements (SLAs) for mitigating vulnerabilities and comply with global regulations with comprehensive visibility into material assets and recommendations to reduce risk. For example, Balbix enables you to gain visibility into all material assets as required by new SEC, DORA, and NIS2 regulations.

Balbix Demonstrates Success in Dollars

Balbix transforms cyber risk assessment for insurance underwriters by offering them a holistic and measurable understanding of an organization's risk landscape, including the successful implementation of the five critical security enhancements sought by underwriters listed on page 10, all presented in financial terms.. Balbix's adaptable dashboards empower organizations to present essential metrics and assess risks in concrete terms, such as dollars or other currencies.



With Balbix's Cyber Risk Quantification (CRQ), insurance underwriters gain access to cyber risks quantified in monetary terms, but tangible evidence of your cybersecurity investments' effectiveness. Instead of abstract technical metrics, you'll present clear, quantifiable data showing how your risk remediation efforts translate into dollars saved.



This transformation from technical jargon to monetary values offers insurers a clear understanding of the potential financial impact of cyber incidents, enabling more informed risk assessment and pricing decisions.

Example: suppose your organization eliminates 85% of its high-impact vulnerabilities that also reduces the likelihood of a data breach by 20%. With CRQ, you can calculate the potential cost savings associated with averting such an incident. This demonstrates to insurers that your cybersecurity initiatives aren't just theoretical — they deliver concrete savings and enhanced security.

Balbix goes beyond surface-level insights by providing traceability from dollars of risk to specific assets and applications driving the risk. This granular visibility allows insurance underwriters to pinpoint the most critical areas of vulnerability within an organization's infrastructure and tailor insurance coverage and premiums accordingly.

Case Study

CARVANA

Security Challenges

Carvana faced significant cybersecurity challenges with high breach likelihood due to a growing backlog of vulnerabilities and outdated software. The use of multiple security tools without proper integration resulted in fragmented data and coverage gaps, complicating vulnerability management and risk communication to the board and executive team.

Solution

Implementing Balbix's AI-driven platform revolutionized Carvana's approach to cybersecurity. Balbix provided comprehensive visibility into vulnerabilities and misconfigurations, assessed threats in real-time, and prioritized remediation based on business impact. This strategic risk management led to a 40% reduction in breach likelihood and a substantial decrease in cyber insurance premiums — saving nearly $250K annually while doubling their coverage.

" Balbix's use of AI isn't just a gimmick like many security vendors. Their use of generative AI, deep learning, and classic machine learning techniques is a core part of the platform, enabling us to deeply understand, quantify, and rapidly reduce our cyber risk across our environment."

Dina Mathers, CISO Carvana

Conclusion:

Securing Premium Reductions Through Strategic Cybersecurity

By strategically integrating robust risk management techniques with savvy insurance negotiations, you position your organization not only as a formidable defender against cyber threats but also as an active participant in the cyber insurance market. Embrace this journey with a focus on making every step measured, effective, and impactful. This guide is your companion in transforming your cybersecurity strategies into tangible, strategic gains, ensuring a proactive posture that aligns with your financial objectives.