DARKReading

TOP TIPS

Overhaul Your Security and Compliance with Integrated Risk Management.

True data protection integrates cybersecurity, privacy, training and the human factor on one unified IRM platform for a holistic view to combat risk.

Across today's security landscape, organizations face constant threats. Multiplying exponentially, these risks carry the potential for catastrophic business failures. In response, companies are jettisoning the siloed approach of single-purpose security tools.

The pandemic revealed the gravity of today's threats: Supply-chain interruptions and data leaks can severely impact your customers, products and brand reputation. But while ransomware and cybersecurity attacks adversely affect operations, Business Continuity (BC) and resilience, they also serve as wake-up calls:

- Are you proactively building a strong risk, compliance, resilience and safety culture?
- Are you ready to grow your business, leave behind cost and infrastructure hassles and eliminate those inefficient, one-off cybersecurity solutions?

Successful companies, from start-ups to enterprises, are choosing a governance, risk management and compliance (GRC) approach to counter persistent threats, protect valuable assets and seamlessly manage an ever-changing regulatory landscape. They're building engaged and empowered corporate cultures committed to security best practices and training their workforce in real time to protect and stay on top of their data.

With these **Top Tips**, we list the critical pitfalls to true security integration and show how you can begin the journey to a holistic cybersecurity approach using a single, unified GRC platform:

1) Prioritize Your SecOps Teams

Unlike marketing, production and management, SecOps teams often lack the comprehensive solutions that can streamline and improve security processes. Provide your SecOps teams with a single-pane GRC platform to manage cyberthreats and vendor risks while providing business continuity (BC). A unified platform ensures that you can take the right risks at the right time with confidence and focus.

2) Confront Vendor Risk

Gain an accurate picture of overall risks since vendor incursions and 3rd party data leaks can quickly become your problems. Suppliers, partners or contractors can introduce vulnerabilities to effective cybersecurity and flawless BC. Take time to understand the threats posed by third-party interconnections — whether you work with 50 or 5000 vendors. Adopt a GRC solution to accelerate analysis through shared libraries of risks, controls and issues.

3) Ensure Organizational Support

C-suite and corporate culture buy-in is vital to successful governance, risk management and compliance. Ensure that the right C-suite alliances and technologies are in place to shift the organizational culture and expand overall threat awareness. Culture change requires patience, diligence and oversight so that new security ideas and approaches are adopted and scale with the organization.

4) Don't Underestimate Risk Levels

Lacking a risk management solution, companies can't be certain they're getting a broad, accurate view of cyber threats and thus underestimate the dangers they face. With an integrated GRC platform, SecOps teams and IT leaders can ensure they're making the best cybersecurity decisions, optimizing budgets and focusing their resources on potential risks that could severely impact their assets and processes.

5) Maintain A Supportive Company Culture

More than just a collection of single-point solutions and an uninformed workforce, effective security requires a corporate culture that's captivated. A unified GRC platform provides pre-loaded frameworks, control libraries, regulatory content and values-based ethics and compliance learning programs so that business teams can stay engaged and empowered.

6) Ensure Business Continuity and Operational Resilience

Natural disasters, cyberattacks, single-point-of-failure breakdowns and application/service outages can be catastrophic for businesses. Multiple siloed tools only limit IT response — they address one problem at a time when there's frequently multiple security issues to tackle simultaneously. With an IRM solution, companies can grow their businesses without cost and infrastructure barriers, align their processes and reduce the time it takes to identify threats along with overall risk.

7) Avoid Budgetary Sinkholes Caused By Overspending

SecOps teams and IT leaders need to be transparent about spending and show how they're contributing to reduce costs as well as operational risks. A holistic IRM platform enables businesses to see upfront the whole spectrum of costs to prevent budget overruns. They can eliminate spending on multiple tools and make accurate predictions on costs and contributions necessary to reduce operational risks.

8) Align Your Cyber Strategy With Business Goals

Show fellow leaders that threat awareness, security protocols and a unified GRC approach are business enablers not obstacles to business growth. Consider whether your organization is adopting the right technologies to improve security and performance through an integrated, single platform.

Conclusion

As the only GRC provider with integrated cybersecurity, privacy and training content, SAI360 simplifies threat mitigation. Integrated risk management doesn't have to be complicated. Or cost prohibitive. SAI360 offers global expertise, learning and best practice content so that organizations can effectively navigate risk. It provides a flexible, agile approach to view governance, risk and compliance standards, achieve risk-ready oversight of business processes and strengthen organizational ethics and employee behavior. To learn more about transforming your security practices, please visit **https://www.sai360.com/solutions/it-risk-cybersecurity**.