From Threat to Recovery:

MANAGING CYBER EVENTS AT EVERY STAGE

BDO

Introduction

In today's digital age, the landscape of cyber risk is constantly evolving, presenting organizations with unprecedented challenges. Traditional methods of safeguarding against cyber threats, such as cyber insurance, are no longer sufficient on their own. To navigate this complex environment, organizations must develop a comprehensive approach to operational resilience. This e-book delves into three critical insights that highlight the importance of preparing for cyber threats beyond conventional means.

Beyond Cyber Insurance: Preparing for Black and Gray Swan Events

The ever-evolving cyber risk landscape demands more than just cyber insurance; it requires operational resilience. Unlike black swans (rare, unpredictable events) and gray rhinos (predictable threats), gray swans are predictable yet poorly understood threats that can cause significant damage if not properly managed.

UNDERSTANDING GRAY SWANS

Gray swans, such as data breaches or ransomware attacks, require organizations to act decisively. Proper training and preparation are crucial for quick, calm, and effective responses. However, many organizations mistakenly believe that basic cybersecurity measures and insurance are sufficient.

THE REALITY OF CYBER COVERAGE

Despite efforts to enhance cybersecurity, many organizations are underinsured. Swiss Re AG reports that less than 20% of organizations have adequate coverage for average ransomware demands. Complacency, driven by a temporary decline in ransomware attacks, can leave organizations vulnerable to future threats.

BEYOND CYBER INSURANCE

Current cyber insurance models often fail to account for the full impact of ransomware attacks, including business downtime and property damage. Organizations need to understand breach scenarios and their forensic costs to prepare effectively.

PREPARING FOR THE INEVITABLE

Organizations should expect breaches and have a detailed playbook ready. This includes assigning roles, alerting necessary parties, and maintaining control during chaotic situations. With insurers scrutinizing cyber hygiene, organizations must meet stringent requirements to avoid higher premiums or lack of coverage.

OPERATIONAL RESILIENCE

True resilience extends beyond IT to include governance, communication, and ongoing maintenance. Companies should assess their cyber capabilities and create a comprehensive roadmap for implementation and upkeep.

Ransomware and other cyber threats are predictable gray swans. As the downward trend in attacks is unlikely to continue, organizations must prepare now. A comprehensive plan, including operational resilience, is essential for effectively handling major cyber events.

READ THE FULL INSIGHT ▶

Considerations for Mitigating the Damage From a Cyberattack

MASTERING CYBER RESILIENCE: KEY STEPS FOR EFFECTIVE RECOVERY

The Growing Threat

Over 80% of organizations have faced multiple data breaches, making a sophisticated resilience plan and structured insurance policy essential. However, even the best plans require effective implementation for successful recovery.

Actionable Steps for Resilience

1. **Develop a Response Playbook:** Develop quick, organized reactions.
2. **Document Everything:** Start as soon as a breach is discovered.
3. **Quantify Losses:** Include business interruptions and additional expenses.
4. **Tailor Cyber Insurance:** Ensure policies meet specific organizational needs.

Immediate Response to Breaches

- **Remove Everyone from the System:** Restrict access to prevent further damage.
- **Secure the Network:** Identify and patch vulnerabilities.
- **Assess the Damage:** Determine the extent and nature of the breach.

Documentation and Reporting

- **Document Key Data Points:** Record business interruptions and additional expenses.
- **Follow Reporting Requirements:** Public companies must file an 8-K form with the SEC; private companies should also disclose incidents to maintain transparency and trust.

Preparing for Effective Recovery

- **Understand Your Insurance Policy:** Know the coverage and limits to avoid unplanned expenses.
- **Quantify Losses Accurately:** Use forensic accountants to document and value losses, helping to ensure proper claims.

Turning Adversity into Advantage

By analyzing breach events and implementing robust policies, organizations can enhance their operational resilience and address high-risk areas. With the right steps, they can turn the negative impacts of a cyberattack into opportunities for improvement.

READ THE FULL INSIGHT ▶

The Return of the Black Swan: How Emerging Technology Will Impact Cyber Risk and Insurance

NAVIGATING THE NEW WAVE OF CYBER RISKS: AI AND BLACK SWAN EVENTS

The Challenge of Emerging Technology

Monumental tech shifts, like the rise of AI, bring unprecedented risks. Organizations must adapt quickly as black swan events—rare, unpredictable occurrences — become more likely.

Dual Risk From AI

Modern technology introduces unknown risks, both from the tech itself and how people use it. AI can create sophisticated phishing attacks and deepfakes, making it easier for cybercriminals to deceive employees.

Steps to Prepare

1. **Align Risk Strategy**: Ensure cohesion across technical, financial, and leadership teams.
2. **Organize Governance Documents:** Maintain business continuity, incident response, and crisis communication plans.
3. **Develop a Cyber Response Playbook:** Prepare for quick, organized reactions.
4. **Oversee Resource Allocation:** Verify that budgets and resources are appropriately managed.

Regulatory Changes

New SEC cyber disclosure rules took effect in December 2023, requiring timely reporting and detailed descriptions of cyber incidents and risk management processes.

Legal Implications

Recent court rulings and SEC enforcement indicate that organizations and individuals could face lawsuits and penalties for data breaches, even if the data isn't misused.

Insurance Considerations

Cyber insurance policies vary widely. Organizations should thoroughly review their policies and consult with professionals to ensure adequate coverage for emerging risks.

Building Strong Policies

To build effective insurance policies, assess terms, conditions, costs, and coverage options. Obtain and evaluate full policy documents before making decisions.

Adapting to Known Threats

As AI and other technologies evolve, organizations will better understand and prepare for cyber threats, improving resilience strategies and insurance policies.

STAY AHEAD

In an era when cyber threats are not just a possibility but an inevitability, organizations must go beyond traditional measures like cyber insurance to ensure their survival and success. This e-book has explored the critical insights necessary for building a comprehensive resilience strategy that addresses the multifaceted nature of modern cyber risks.

1. **Beyond Cyber Insurance:** Operational resilience is crucial for handling gray swan events, which are predictable yet often mishandled threats. Organizations must extend their resilience efforts beyond IT to include broader operational aspects.
2. **Mitigating Cyberattack Damage:** Effective resilience plans and well-structured insurance policies are essential but not sufficient. Organizations must also focus on the implementation of these plans, documentation of losses, and understanding the nuances of their insurance coverage.
3. **Emerging Technology and Cyber Risk:** The rapid advancement of technologies like artificial intelligence introduces new, unpredictable risks. Organizations must align their risk strategies across technical, financial, and leadership teams to prepare for these black swan events.

As cyber threats continue to evolve, so must your organization's approach to risk management and resilience. Don't wait for a cyber incident to expose vulnerabilities in your current strategy. Take proactive steps today to fortify your defenses and ensure your organization is prepared for whatever the future holds.

SCHEDULE A MEETING WITH BDO

BDO is here to help you navigate the complexities of cyber risk and build a robust resilience strategy. Our team of experienced professionals can assist you in:

- Developing comprehensive operational resilience plans
- Structuring and enhancing your cyber insurance policies
- Implementing effective response playbooks
- Quantifying losses and navigating the claims process
- Understanding and preparing for emerging technology risks
- Take the first step toward a more resilient future by reaching out to BDO and letting us help you build a strategy that not only protects your organization but also positions it for long-term success in the face of cyber uncertainty.

READ THE FULL INSIGHT ▶

HAVE QUESTIONS OR WANT TO LEARN MORE? **CONTACT US!**

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.