The tech chronicle

Sirtawn Systems

Start Fighting Cyber Crime with Knowledge and Action.

Our Newsletter for Issue #172 is dedicated to Cyber Risk Assessment.

Why you need a Cyber Risk Assessment Program

Today's Top Cyber-Risks:

Phishing attacks
Emails and messages.

Ransomware attacks
Malicious Software to lock data hostage.

Data breaches
Unauthorized Individuals gain access to sensitive information.

Insider threats
Your employees, intentionally or unintentionally compromise.

Supply chain Vulnerabilities
IT infrastructure of suppliers can be manipulated to hack your business.

Social engineering attacks
Manipulative tactics used to deceive individuals.

Distributed Denial-of-Service attacks
Coordinated attacks to overwhelm systems with traffic.

Potential Impacts Of Cyber Incidents:

- **Financial loss** – Your business could suffer heavy financial losses through theft, fraud and associated remediation expenses.
- **Reputational damage** – Cyber incidents damage your brand's image, erode customer trust and ultimately affect your business growth.
- **Business disruption and downtime** -- Disruption to your day-to-day operations can cause significant downtime, reduce productivity and cause revenue loss.
- **Legal liabilities** – Your business may face compliance woes, including lawsuits, for failing to protect sensitive customer data.
- **Supply chain disruptions** – Cyber incidents can trigger disruptions that can cause delays in production and delivery, resulting in unmet customer expectations, revenue loss and potential long-term damage to your business relationships with suppliers and customers.
- **Loss of competitive advantage** -- Your business could lose its competitive edge due to the loss of intellectual property, such as patents, trade secrets or innovations.

THE FOUR STAGES OF CYBER RISK MANAGEMENT

Although eliminating cyber-risks completely may be impossible, a comprehensive cyber risk management strategy can help address your organization's critical security gaps, threats and vulnerabilities, reducing overall risk.

THE FOUR STAGES UNVEILED

Risk identification

IDENTIFY

- Recognize vulnerabilities susceptible to cyberthreats.
- Conduct a thorough risk assessment.
- Consider internal and external factors.
- Classify assets based on importance and sensitivity.

Risk assessment & analysis

ASSESS

- Evaluate identified risks for potential impact and likelihood.
- Analyze consequences and assess the probability of occurrence.
- Estimate financial, operational and reputational impact.
- Prioritize risks based on significance to the organization.

Risk mitigation & control

MITIGATE

- Develop strategies to mitigate identified risks.
- Implement controls to reduce likelihood and impact.
- Enforce cybersecurity policies and Procedures.
- Conduct regular assessments and address gaps.

Monitoring & review

MONITOR

- Continuously monitor risk mitigation Measures.
- Adapt the plan to evolving threats.
- Keep an eye on any deviations from the normal.
- Regularly review and update the plan.

Need help implementing a cyber risk management program?

Contact Sirtawn Systems Today!

How Effectively Managing Risk Bolsters Cyber Defenses.

In today's rapidly evolving digital landscape, where cyberthreats and vulnerabilities continually emerge, it's obvious that eliminating all risk is impossible. Yet, there's a powerful strategy that can help address your organization's most critical security gaps, threats and vulnerabilities — comprehensive cyber risk management.

Implementing a well-thought-out cyber risk management strategy can significantly reduce overall risks and strengthen your cyber defenses. To understand the profound impact of this approach, continue reading as we delve into the nuances that make it a game changer in digital security.

Cyber risk management vs. traditional approaches

Cyber risk management diverges significantly from traditional approaches, differing in the following key aspects:

Comprehensive approach: Cyber risk management isn't just an additional layer of security. It's a comprehensive approach that integrates risk identification, assessment and mitigation into your decision-making process. This ensures there are no gaps that could later jeopardize your operations.

Beyond technical controls: Unlike traditional approaches that often focus solely on technical controls and defenses, cyber risk management takes a broader perspective. It considers various organizational factors, including the cybersecurity culture, business processes and data management practices, ensuring a more encompassing and adaptive security strategy.

Risk-based decision-making: In traditional cybersecurity, technical measures are frequently deployed without clear links to specific risks. Cyber risk management, however, adopts a risk-based approach. It involves a deep analysis of potential threats, their impact and likelihood, allowing you to focus technology solutions on addressing the highest-priority risks.

Alignment with business objectives: A distinctive feature of cyber risk management is its alignment with your overarching business objectives. It ensures that your cybersecurity strategy takes into account your mission, goals and critical assets, thereby making it more relevant to your organization's success.

Holistic view of security: Cyber risk management recognizes the significance of people, processes and technology, embracing a holistic view of security. It acknowledges that a robust security strategy is not solely dependent on technology but also on the people implementing it and the processes that guide its deployment.

Resource allocation: By prioritizing risks based on their potential impact and likelihood, cyber risk management allows you to allocate resources more effectively. This means that your organization can focus on the areas of cybersecurity that matter the most, optimizing resource utilization.

Key Components of Risk Tolerance:

- **Willingness to take risks -- Reflects how much risk an organization is willing to take to achieve its objectives.**
- **Expectations of customers and stakeholders -- Considers the preferences and expectations of customers and stakeholders to maintain trust and support.**
- **Strategic objectives and long-term goals -- Ensures that risk management is aligned with the organization's business-critical objectives and long-term growth plans.**

- **Compliance and regulatory considerations -- Involves adhering to legal and regulatory standards to mitigate compliance-related risks.**
- **Ability to absorb loss -- Shows an organization's ability to bear financial losses and continue operations.**

How to achieve cyber risk assessment success:

1. Perform a digital inventory
Gain a comprehensive understanding of your IT environment by identifying and classifying all business-critical assets.

2. Stay Informed
Knowledge is your strongest defense. Keep yourself updated and well-informed on evolving cyberthreats and vulnerabilities.

3. Identify your weaknesses
Frequently perform vulnerability assessment scans to identify and correct weaknesses malicious actors could exploit.

4. Conduct an impact analysis
Evaluate the likelihood of each identified vulnerability and gauge the potential financial impact on your business.

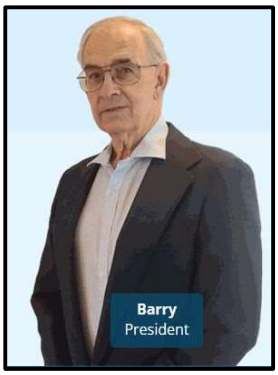
5. Prioritize threats by degree of risk
Rank the threats based on their likelihood and impact on your business. It will help you allocate resources efficiently and focus on the most critical risks.

6. Develop an action plan
Create an action plan that strategically outlines how to manage and mitigate risks based on their priority levels.

7. Document everything
Record all the identified risks and your mitigation strategies for continuous monitoring and risk management.

Gain a competitive advantage without losing sight of security.

Our Assessment Offer



This monthly publication provided courtesy of Barry Brown, President of Sirtawn Systems.

FIGHTING CYBERCRIMINALS ON YOUR OWN CAN BE TIRING WHEN YOU HAVE A BUSINESS TO RUN.

CONTACT US TODAY

FIND OUT WHAT IT'S LIKE TO HAVE OUR CYBERSECURITY EXPERTS IN YOUR CORNER.

We are offering a FREE Network Security Audit with no obligation. You will receive a "Cyber Security Audit" outlining our findings following the audit. Again … **NO Obligation….**

Sirtawn Systems
Your Cyber Security Experts

Phone: (905) 947-1636
Website: www.sirtawn.com
Email: sirtawnsystems@gmail.com