9 WAYS TO OPTIMIZE:
A CYBER RISK ASSESSMENT CHECKLIST

Protect your organization from cyber attacks. Assessing cyber risk exposure can help you model operational risks, and manage them more effectively.

As you gain new insights into your IT infrastructure, you'll be able to:

- Ensure compliance with regulatory and legal mandates
- Make more informed investment decisions
- Provide peace of mind for clients and shareholders
- Understand the efficacy of your risk management initiatives
- Develop a stronger overall cyber security posture

And more.

This checklist provides you with a high-level overview of actionable steps to take in optimizing business security decisions, solving challenges, and driving long-term business growth.

1 Identify business assets.

Recognizing the type of valuables that your organization must safeguard is key in assembling effective policies, and implementing the right cyber security software. Make note of the servers, websites, proprietary information and client/customer data that requires protection. In addition, get rid of data that you don't need. Criminals cannot steal what they cannot see.

2 Anticipate the threats.

How would a cyber criminal attempt to gain access to your resources? Vulnerabilities can be physical (think badge access) or they can be virtual, as in the case of unpatched applications, expired certificates or lack of a firewall. Where are your security gaps?

3 Calculate the probabilities.

Based on the architecture that you have in place, and the accompanying security, how likely are hackers to get into your system? After evaluating, engage in cross-team collaboration to determine how to reduce the probability of incidents.

4 Consider the repercussions.

Explore different cyber breach scenarios, and examine the types of harm that they could inflict. Data loss, legal issues and regulatory penalties, system or application downtime... etc. Can your organization comfortably contend with the consequences?

5 Controls in place.

Do you have security policies? Are you keeping your policies updated? How about employee cyber threat awareness training? Modern security software? Investing in modern, up-to-date software is absolutely critical in terms of improving security.

6 Enforce least-privilege access.

Provide employees with the access that they need, but avoid providing higher levels of access than necessary. Periodically review access privileges.

7 Publish an incident response plan.

When an attack hits, know who's going to handle internal communications, where contact information can be found, where to find emergency tech tools, and how you'll manage the PR side of things. These are incident response plan basics. More information on developing an incident response plan can be found here.

8 Strategic IT infrastructure improvements.

Ensure that your organization keeps pace with the ever evolving threat landscape. Make a point of regularly reading about new products and conduct quarterly audits of your infrastructure to determine what could be upgraded. Execute on findings.

9 Establish a recovery process.

Determine how your organization will retrieve lost data. Do you have a full-disk encrypted backup system? Will you rely on third-party data recovery services?

Make sure that your organization is secure. Build a cyber resilient workplace through comprehensive consideration of the aforementioned concepts, and through the application of best practices.

For more information about managing your cyber risk, read our whitepaper.