cyberconIQ

Top 5 +5 Bonus Questions CISO's Need Answers to in 2022.

Security Leaders in General!

Discover how cyberconIQ can help.

Top 5 Questions CISO's Need Answers to in 2022.

Discover how cyberconIQ can help.

1. **What is our cybersecurity strategy, and does it address business risk? How?**

   Leveraging our deep expertise and deploying our patent-pending solutions and security frameworks, we work with you to focus on a risk-based approach that first helps identify your organization's challenges and prioritize your needs and current cybersecurity maturity level with an actionable and achievable strategy.

2. **Are my employees properly trained?**

   Through its patented research, cyberconIQ offers a full suite of SaaS based solutions that are proven to measurably reduce the probability of a human factor's cybersecurity breach. Operating at the intersection of cybersecurity and psychology, cyberconIQ embeds proven behavioral science methods targeting changes in on-the-job behavior. Our continuous education platform offers personalized and effective micro learning modules throughout the year that keep employees up to date on the most recent threat vectors that are specific to their risk-style.

3. **If we were hit by a major attack, how confident are you that we could recover quickly?**

   We understand the importance of cyber resiliency, which is why you prepare and train for potential cyber incidents or attacks. Even the best Incident Response Plan (IRP) needs to be assessed and re-evaluated as threat landscapes evolve, new employees start and your environment changes. We offer a interactive tabletop exercise that addresses these complexities in a cost effective and efficient IR Planning session.

4. **How do you measure and manage our cybersecurity program?**

   Our breakthrough approach and Cyber Risk Dashboard allow you to effectively lower total organizational probability and costs associated with a cyber breach by understanding the unique makeup, or "cyber DNA", of your organization using three simple steps to measure and manage your people, process and technology.

5. **How do you determine what percentage of the IT budget is allocated for cybersecurity?**

   We understand that a cybersecurity budget could be endless. Through our Advisory Services we help you focus on high impact strategies that strengthen your organization. The proposed budget isn't just routinely spent to check boxes, through our research, it is focused on what works to protect your organization.

Data Breach Statistics for 2021 - Key Takeaways

Ransomware Still on the Rise

Appearing in 10% of breaches - more than double from 2020.

The Human Element

85% of breaches involve the human element. Breaches caused by phishing were also up 25%.

Business Email Compromise

The second-most common form of social engineering leading to a cyber breach.

*Source: Verizon DBIR, 2021 Data Breach Investigations Report - https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf

BONUS 5 Questions CISO's Need Answers to in 2022

Discover how cyberconIQ can help.

1. **Do we have the right policies and do our employees understand them?**

   Policies are a foundational starting point for any cybersecurity program. But do you have the right policies in place? Most CISO's may answer yes, but how do they know? Who assisted you with the selection, the writing, and the implementation of the policies as it relates to your industry and threat landscape?

2. **Do I know where our confidential data is and is it protected?**

   You can't protect what you don't know or know you have. A thorough understanding of what data you are collecting and where it sits is a key question all CISO's should know the answer to, but most don't. Our Advisory Service's Cybersecurity Playbook is customized to your organization and in the playbook we spend a considerable amount on classifying and identifying your data.

3. **Can you demonstrate how you are following best practice frameworks?**

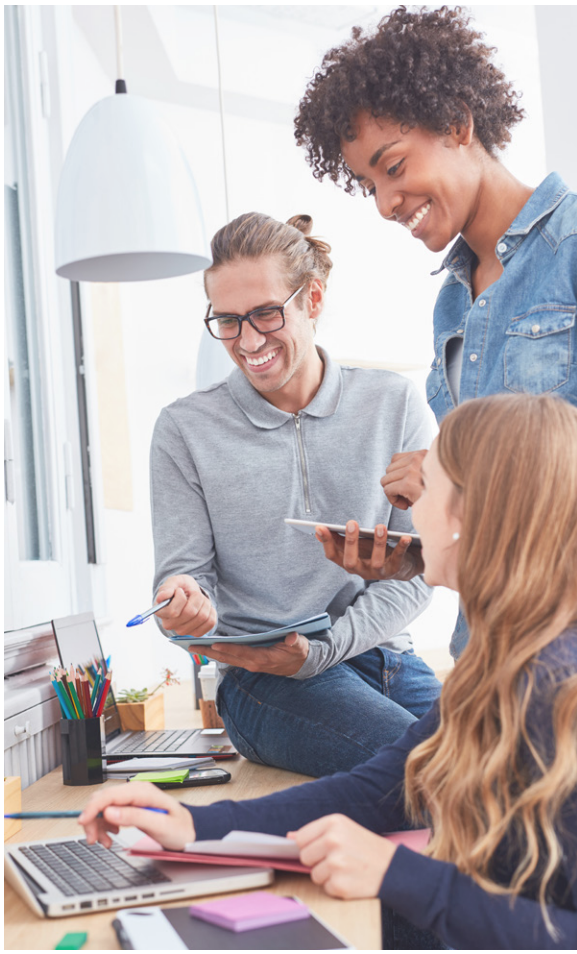
   We understand every organization has unique compliance and regulatory requirements. Our Advisory Services team begins by listening to your priorities and proposes actionable and achievable strategies to close the gap in your current cybersecurity controls and program maturity level. From standards selection (NIST, CIS, ISOx etc), to implementation strategy, we'll be there to guide your team along the way.

4. **Does our resilience strategy address the changing risk landscape?**

   Year after year the risk landscape changes, and you must adapt because to do nothing or do continue doing the same isn't acceptable. Our cybersecurity playbook will arm you with a necessary roadmap to navigate the changing risk landscape.

5. **How do we manage our supply chain threats?**

   2021 taught us that assessing our supply chain is as important as assessing our own cybersecurity program. You need a policy on reviewing service providers, an inventory of these vendors, and a risk rating associated with their potential impact to the business in case of an incident. You also need to check for language in contracts to hold them accountable if there is an incident that impacts your organization.



About cyberconIQ

cyberconIQ offers a full suite of SaaS based products and advisory services that are proven to measurably reduce the probability of a human factors cybersecurity breach. cyberconIQ embeds proven behavioral science methods targeting changes in on-the-job behavior into all of its Cybersecurity Products and Risk Advisory Services as a market differentiator.

Enhance your organizational resilience today!

Book your demo at cyberconIQ.com.