BDO KNOWS:

CYBERSECURITY

WHAT CEOS SHOULD KNOW & DO ABOUT CYBERSECURITY

During the past few months, we have spoken with hundreds of companies Chief Executive Officers (CEOs) from numerous U.S. and global industries, including financial services, healthcare, government contracting, automotive, manufacturing, private equity, and law firms, about the importance of cybersecurity. From these conversations, we've concluded that the three most frequently asked questions by CEOs are:

1. What should we know about cybersecurity?

2. What should we do about cybersecurity?

3. How do we assess the quality of our cybersecurity program?

CONTACT

GREGORY GARRETT
Head of U.S. & International Cybersecurity
703-770-1019
ggarrett@bdo.com

It is vital that CEOs establish the appropriate cybersecurity "tone at the top" for their respective organization, regarding the importance of information security and how cybersecurity is everyone's shared responsibility in a truly digital world. Establishing an organizational "culture of cybersecurity" has proven to be one of the best defenses against cyber adversaries. It is the people, not the technology, which can either be an organization's greatest defense, or its weakest link against a cyber-attack.

Further, it is incumbent upon CEOs to learn more about cybersecurity to ensure their company is taking appropriate actions to secure their most valuable information assets. This does not mean that every CEO needs to become a Certified Information System Security Professional (CISSP). Rather, CEOs should increase their knowledge of core cybersecurity concepts and leverage their own leadership skills to conceptualize and manage risk in strategic terms, understanding the business impact of risk.

FIVE THINGS CEOS SHOULD KNOW ABOUT CYBERSECURITY

1. Cyber-attacks and security breaches **will** occur and **will** negatively impact your business. Today, the average cost of the impact of a cyber breach is $4.9 million.
2. According to most cybersecurity surveys, over 60% of all data breaches originate from unauthorized access from one of your current or former employees, or third-party suppliers.
3. Achieving information security compliance with one or more government regulatory standards for information security (i.e. ISO 27001, NIST 800-171, HIPAA, NYDFS, etc.) is good, but not sufficient to ensure real cybersecurity.
4. Cyber liability insurance premiums are significantly increasing in cost and often do not cover all of the damages caused by a cyber breach.
5. To achieve real information security and data resilience it is vital to combine managed Monitoring, Detection, and Response services with comprehensive disaster recovery and business continuity plans.

TEN THINGS CEOS SHOULD DO ABOUT CYBERSECURITY

1. Ensure everyone in the organization from the top-down receives appropriate cybersecurity education and awareness training.
2. Hire an independent company to conduct a cyber risk assessment against government regulatory compliance requirements and industry standards to identify potential gaps in your company's information security policies, processes, plans, and procedures.
3. Verify that periodic penetration testing by certified Ethical Hackers is being conducted to identify potential cybersecurity vulnerabilities in your organization's information systems.
4. Require a timely and effective software patch management program be implemented by your Information Technology team to mitigate known security vulnerabilities as quickly as possible.
5. Ensure the organization has 24/7/365 monitoring, detection, and response capabilities for its information systems.
6. Verify the organization has an appropriate cyber breach incident response plan, including the policy and procedures related to ransomware attacks.
7. Hire an independent firm to conduct a cyber liability insurance coverage adequacy evaluation.
8. Establish information security key performance indicators (i.e. number of cyber-attacks, number of data breaches, network uptime, network downtime, cost of cyber breaches, cost of cyber insurance, cost of information security as a percentage of total company IT cost, etc.).
9. Ensure your company has well-documented and periodically tested disaster recovery and business continuity plans to quickly recover lost or stolen data to mitigate potential damages of cyber breaches.
10. Mandate additional layers of information security via encryption, multi-factor authentication, and highly restricted access to your company's most valuable information assets.

SEVEN STRATEGIC QUESTIONS A CEO SHOULD ASK TO BEGIN THE PROCESS OF ASSESSING THE QUALITY OF THEIR CYBERSECURITY PROGRAM

1. What is the threat profile of our organization based on our business model and the type of data our organization holds?
2. Who may be after our data - Nation States, sophisticated international criminal organizations, or ideologically motivated hacktivists?
3. Does our cybersecurity strategy align with our threat profile?
4. Is cybersecurity risk viewed as an enterprise-wide risk issue and incorporated into the overall risk identification, management and mitigation process?
5. What percentage of our IT budget is dedicated to cybersecurity? Does it conform to industry standards? Is it adequate based on our threat profile?
6. Is there someone in our organization dedicated full-time to our cybersecurity mission and function, such as a Chief Information Security Officer?
7. Is the cybersecurity function properly aligned within our organization? Aligning the CISO under the CIO may not always be the best model as it may present a conflict. Many organizations align this function under the risk, compliance, audit or legal functions - some with direct or "dotted line" reporting to the CEO.

It has become abundantly clear that some CEOs simply do not know enough about cybersecurity and that their Chief Information Officers and Chief Information Security Officers do not always provide them with an accurate portrait of the cyber risks which their company is facing every day. Other CEOs appear to be suffering from a "knowing" versus "doing" gap. From our consulting experience and research, we understand that many CEOs are well aware of the cyber risks, but for one or more reasons, often short-term financially motivated, they are choosing not to do what needs to be done in order to reduce the probability and/or impact of a cyber breach in their organizations. In the world of cybersecurity the old adage is quite true "You can pay now, or you can pay much more later!"