BDO KNOWS:

CYBERSECURITY

WHAT CFOS SHOULD KNOW & DO ABOUT CYBERSECURITY

The tone at the top of every organization is critical to success. In the digital age where millions of electronic devices are linked to the Internet nearly every day, forming the Internet of Things (IoT), cybersecurity awareness is vital for everyone in the organization. Since senior executives have the greatest access to the most valuable information, it is essential that they receive appropriate cybersecurity education and training. Unfortunately, most Chief Financial Officers (CFOs), other members of the C-Suite, and Boards of Directors (including Audit Committees) of many organizations are not as knowledgeable about cybersecurity as they should be, and that is an area of significant concern.

CONTACTS:

GREGORY GARRETT
U.S. and International Cybersecurity Advisory Services Leader
703-893-0600
ggarrett@bdo.com

MIKE STIGLIANESE
Managing Director, Cybersecurity Advisory Services
212-817-1782
mstiglianese@bdo.com

GREG SCHU
Partner, Cybersecurity Advisory Services
612-367-3045
gschu@bdo.com

WHAT CFOS SHOULD KNOW & DO ABOUT CYBERSECURITY

Based upon discussions conducted in 2018 with numerous Chief Financial Officers (CFOs) from various industries, including financial services, healthcare, government contracting, automotive, manufacturing, private equity, and law firms, it appears there exists a real gap in both knowledge and proactive actions to enhance cyber defense. From these conversations, the three most frequently asked questions by CFOs were:

1. What should CFOs know about cybersecurity?
2. What questions should CFOs ask Chief Information Officers (CIOs) and General Counsels (GCs) about cybersecurity?
3. What should CIOs do about cybersecurity?

It is vital that CFOs establish the appropriate cybersecurity "tone at the top" for their 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 CFOs 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 CFO needs to become a Certified Information System Security Professional (CISSP). Rather, CFOs should increase their knowledge of core cybersecurity concepts, and leverage their own leadership skills to conceptualize and manage risk in strategic terms about how best to invest their time and resources to improve cyber defense.

TOP TEN THINGS CFOS SHOULD KNOW ABOUT CYBERSECURITY

1. What are the organization's most valuable digital assets? Cyber-attacks and security breaches will continue to occur and will negatively impact the business. Today, the average cost of the impact of a cyber breach is $7.5 million according to the U.S. Security Exchange Commission (SEC).

2. How much cyber liability insurance coverage is necessary to financially protect the company's assets?

3. What is our organization's risk of a cyber breach? According to most cybersecurity surveys, over 60% of all data breaches originate from unauthorized access from one of the organization's current employees, former employees, or third-party suppliers.

4. Has the organization created an insider-threat program to mitigate the risk of a cyber breach from within the organization?

5. What actions should our organization take to ensure real cybersecurity? Achieving compliance with one or more government regulatory standards for information security (i.e. ISO 27001, NIST 800-171, HIPAA, NYDFS, AICPA-SOC, etc.) is good, but not sufficient to ensure real cybersecurity.

6. Has the organization had an independent email and network threat assessment recently conducted? If so, then what were the results?

7. Have we had an independent assessment of the adequacy of our cyber liability insurance coverage? Cyber liability insurance premiums are significantly increasing in cost and often do not cover all of the damages caused by a cyber breach.

8. Do we have the internal resources to perform MDR (Monitoring, Detection, and Response) work or do we need to outsource these efforts? If so, then how much will it cost? To achieve real information security and data resilience it is vital to combine managed MDR with Managed Security Services (MSS).

9. Does the organization have a comprehensive incident response (IR) plan, disaster recovery (DR) plan, and business continuity plan (BCP)?

10. If we are attacked by ransomware, are we going to pay the ransomware? If so, then how much should be budgeted? Will it be covered by cyber liability insurance coverage?

TOP TEN QUESTIONS CFOS SHOULD ASK CIOS & GCS ABOUT CYBERSECURITY

1. What is the organization's overall risk of a data breach in terms of both probability of occurrence and financial impact?
2. How much cyber liability insurance coverage does the organization need to protect the organization's financial interest?
3. What is the average cost of a cyber data breach in our respective industry?
4. What are the financial penalties for failure to fully comply with cybersecurity industry specific regulatory requirements?
5. What is the cost of compliance as it relates to the cybersecurity industry requirements and/or specific contract/subcontract requirements?
6. Is it better financially to insource or outsource necessary cybersecurity hardware, software, and professional services?
7. Whom can we trust to advise the organization if a significant cyber-attack and data breach occurs?
8. What information regarding cybersecurity risks and mitigation actions should be reported to the board of directors?
9. Does the organization have the right people to make informed business decisions about cybersecurity?
10. Does the organization need to engage outside cybersecurity technical consultants and/or outside counsel with more experience in cyber incident response and cyber claim preparation and processing?

TOP TEN THINGS CIOS SHOULD DO ABOUT CYBERSECURITY

1. Work with the CEO, CFO, and/or Board of Directors to hire a dedicated, well educated, experienced, certified information technology and cybersecurity professional to serve as the Chief Information Security Officer (CISO), if possible.
2. Hire independent firms to periodically conduct the following: email cyber threat assessments, network cyber threat assessments, vulnerability assessments, penetration testing, and targeted spear-phishing campaigns all designed to gather data on the real state of the organization's current level of cybersecurity.
3. Work with the rest of the C-Suite to assess cyber risks from every functional area of the organization.
4. Create an appropriate budgetary balance between information technology, information governance, risk, security, and compliance.
5. Ensure an appropriate data privacy program and insider-threat program.
6. Verify a timely and effective software patch management program.
7. Ensure appropriate information access, storage, dissemination, and business continuity.
8. Work to create an organization –wide cybersecurity culture.
9. Outsource the 24 x 7 x 365 Monitoring, Detection, and Response (MDR) services to a qualified and experienced Managed Security Services Provider (MSSP).
10. Ensure timely reporting of all data breaches.

CONCLUSION

It has become abundantly clear that some CFOs simply do not know enough about cybersecurity, and their C-Suite executive counterparts (including the CEO, COO, GC, CIO, and CISO) do not always provide them with an accurate portrait of the cyber risks their company is facing every day. Other CFOs appear to be suffering from a "knowing" versus "doing" gap. It is clear that many CFOs 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.