W H I T E P A P E R

Director to Director

Briefing Series

Cybersecurity: Getting to 'The Truth'

The Definitive Protocol for Directors to Effectively Lead

Facilitating the Director's Active Oversight Role in Cybersecurity

April 2016

Director to Director

Briefing Series

Cybersecurity: Getting to 'The Truth'

Cybersecurity has rapidly become the top agenda item with company boards across the U.S. and throughout the world. In terms of risk, cybersecurity represents the most significant and dangerous risk in its potential to immediately damage reputation and financial standing for both directors personally and the companies they serve.

The U.S.economy (through U.S. companies) loses $5 trillion in value each year due to theft of trade secrets and sensitive data; representing 1/3 of the U.S. GDP. Much of this stolen innovation is identically re-created overseas then sold back to U.S. customers at less than 50 cents on the dollar. When the intelligence is analyzed, U.S. companies have been in the center of a maturing information and economic war for many years. Cybersecurity is a matter of national security.

Most directors did not come up through the IT or cyber ranks and even those who did feel like they are fighting a ghost or more accurately, many ghosts. This is due to the increased complexity through an exponential increase in breach activity by nation-states and and privateer hackers. Adding to the confusion, is the constant onslaught of new cybersecurity companies with limited protection capabilities led by the venture capital community; offering an equal number of different views of the cybersecurity market and their proposed 'fix'.

With IT budgets historically increasing 12% year over year and data breaches up over 400% this year alone, directors have come to find it difficult to trust their own staff and cybersecurity vendors with their view of the path forward. Recent reported breaches represent only 10% of the actual number of breaches due to federal reporting requirements on Personally Identifiable Information (PII). With respect to the remaining 90%, many companies either do not report or worse, don't know they have been breached.

As with any board issue or crisis, we must begin by building our problem-solving on a foundation of facts. In cybersecurity, this is extremely difficult due to the factors previously stated. Following are the unvarnished facts directors are seeking:

The fix to cybersecurity is solely a board-level issue. It requires a policy change, a culture change, and a funding allocation change - this can only occur at the board level. In other words: a transformation. There are many hurdles internally to overcome: communication gaps, separate agendas, territorial silos, denial, complacency, contractors, suppliers, partners, law firms, and so on. The task of immediately engaging and completing a transformation into data protection relates directly to company survival.

Through extensive intelligence, we must understand that data breaches are not random, rather, part of a decades-long policy of two primary nation-states and a number of privateer hackers. To truly develop an effective cyber strategy, we must first understand our adversary and their true motivation and capability behind the attacks and successful breaches.

All credible intelligence points to the same unmistakeable conclusion: cybersecurity technologies are fractionally adequate driving an insider threat and sensitive data protection strategy as the keystone in the path forward. Companies have placed blind faith in IT and cybersecurity technology as a complete solution at a significant loss to true protection. In a recent article, the president of computer and network security company RSA stated: "Cybersecurity industry is fundamentally broken." http://www.scmagazine.com/rsa-cyber-security-industry-is-fundamentally-broken-says-amit-yoran/article/451625/

To further illustrate: U.S. government agencies spent $86 billion in cybersecurity last year only to experience two White House breaches, two IRS breaches, two State Department breaches, two OPM breaches, a CIA Director breach; these are only the breaches they know about. One insider threat can gain superior access to sensitive data and render all cybersecurity efforts worthless; proven by over 95% of all data breaches are facilitated by human intervention. (Insider threat includes employees, ex-employees, interns, contractors, vendors, suppliers, partners, and law firms)

Cybersecurity remains important, but takes a backup position behind insider threat and sensitive data protection.

With respect to cybersecurity, directors have the fiduciary duty to:

- Reduce Risk
- Limit Liability (both personal and corporate)
- Active Oversight

Reducing Risk Limiting Liability Active Oversight

Director Cybersecurity Checklist and Next Steps

The following checklist represents the latest developments in comprehensive director protective cybersecurity actions. Each action must be executed with the premise that a breach has occurred.

1 **Perform an annual board legal vulnerability assessment by a leading specialized cyber law firm**

- Identify legal vulnerabilities in advance and significantly reduce exposure before, during and after a data breach
- Performed under complete confidentiality
- Traditional brick and mortar, 'one size fits all' law firms are not recommended for this exercise

2 **Perform biannual data breach exercises with the entire C-level**

- Data breaches are occurring with unprecedented frequency and will continue to occur in every company
- Secure a leading third-party firm as an unbiased facilitator, firm cannot represent cybersecurity products or other competing or conflicting services
- Must be in extensive detail and fully documented by each functional group and reviewed by facilitator
- Board to be involved in 'hot wash' review of the exercise and summary key performance indicators (KPI's)

3 **Perform annual board cyber vulnerability assessments facilitated by a leading specialized cyber firm**

- Identify cyber vulnerabilities in advance and significantly reduce exposure before, during and after a data breach
- Performed under confidentiality in conjunction with legal vulnerability assessment
- Firm must be unbiased and cannot represent cybersecurity products or other competing or conflicting services

4 **Perform a company-wide transformation to data-centric security with emphasis on insider threat**

- Secure a leading third-party firm as an unbiased facilitator, firm cannot represent cybersecurity products or other competing or conflicting services
- Utilize a strategy-specific methodology to facilitate the transformation
- Include all employees, contractors, vendors, suppliers, partners and law firms

5 **Require cybersecurity updates at each board meeting separately by CIO, CISO and Risk executive**

- Include cybersecurity questions from page three of this document
- Include intelligence-based events and decisions
- Include preset KPI matrix

6 **Place a cybersecurity director on the board or have a leading unbiased firm act as an advisor to the board**

- Must have both recent enterprise cyber and intelligence experience

Reducing Risk Limiting Liability Active Oversight

Director Cybersecurity Questions for the CIO, CISO, CSO and Risk Executive

The following list of director questions are for the CIO, CISO, CSO and Risk executive to be asked immediately. They are central to the efficacy of an effective cyber security program and fostering a unified team. Each should be fully documented with ownership, action plans and status updates at each board meeting.

1. Do we have a documented cyber security strategy? Is it strictly followed at all levels? What are the exceptions?
2. Do we have a documented data breach exercise at the C-level? Is it comprehensive with a 'go team', emergency contacts, cyber law firm, regulators, law enforcement, PR firm with steady templates, etc.? Is it executed biannually by an unbiased and qualified third-party?
3. Do we have an ongoing data classification program to identify levels of our sensitive data?
4. Are the results of our data classification program fed into our data protection strategy?
5. Where is each level of our sensitive data stored?
6. How is our 'Tier 1' sensitive data protected and managed?
7. Who has access to our sensitive data? How are they using it?
8. How is access managed?
9. Where is our sensitive data going?
10. How are we limiting access to 'need to know only'?
11. How do we limit damage to our reputation?
12. How do we protect our reputation?
13. How are we using cyber liability insurance to transfer risk?
14. Do we have a documented sensitive data protection strategy?
15. What are our current policies for ongoing training and handling of insider threat? Is it comprehensive and does it include all employees, new hires, contractors, interns, suppliers, vendors, partners and law firms?
16. Do we have biannual cybersecurity awareness training and certification conducted by a leading firm? Is it updated with current intelligence? Does it include all employees, new hires, contractors, interns, suppliers, vendors, partners and law firms?
17. Do we have a reward-based system for finding any sensitive data security vulnerabilities?
18. Do we deploy an external expert white hat 'red team' attempting to hack our network? What are the results?
19. Do we use a third-party 'red team' to counter insider threat?
20. Do we deploy active DarkNet management for advanced warning and resolution of nefarious activity?
21. Do we have documented boundaries of our interconnected enterprise with network topologies including wireless, remote and cloud access? Does it include all of our third-parties including our law firms?
22. How do we identify unusual network or user activity across our network and extended supply chain? Are our hosted, remote and cloud environments included?
23. Is there a designated cross-functional risk management team with specific objectives who meet regularly?

Corporate Headquarters
BLACKOPS Partners Corporation
2200 Pennsylvania Avenue NW, 4FL East
Washington, DC 20037
+1.202.888.4991 - Directors Only
www.blackopspartners.com
contact@blackopspartners.com

BLACKOPS® PARTNERS

BLACKOPS Partners Corporation - trusted Cyber Advisors to the senior leadership of the world's largest companies and institutions. Strategically teamed Cyber Board includes the top senior thought leaders from the CIA, FBI, US Secret Service, IBM Global Services, Deloitte Consulting, McAfee, EDS and others.