How to Increase Your CEO and Board's Cybersecurity Literacy

T. Casey Fleming, CEO
BLACKOPS Partners Corporation

Anthony M. Chapa, Director
BLACKOPS Partners Corporation
Former Assistant Director and Chief Technology Officer, U.S. Secret Service

Current State

As 2015 unfolds, cybersecurity is the hot topic in boardrooms today. According to Forbes, 2014 was the year of the data breach, and we would be wise to brace for more in 2015.[1] FireEye CEO Dave DeWalt stated, "The trend of massive data breaches are now the new norm as 97% of companies are currently being hacked."[2] The FBI warned that data breaches are up 400%, and a doubling or tripling of the available workforce to counter them may be required.[3] Looking into the near future, *Corporate Counsel* recently stated that if the current trend continued, breaches were on track to cost companies $2.1 trillion.[4] This trend illustrates the fact that the CEO and board of every U.S. company needs an immediate new cybersecurity game plan, beginning from the top down.

Company-Wide Effort

The board's role in cybersecurity is defined as active oversight. Directors, officers, and CEOs can be held personally liable for failing to appropriately monitor and supervise the enterprise, including the protection of sensitive data. According to a recent article by *Chief Executive*, "While the mechanics of identifying and remediating attacks may reside with the IT team, cybersecurity has become a company-wide effort that the leadership team must oversee."[5]

As a result of recent breaches, boards have realized that cybersecurity is no longer just an IT problem; it is a business risk problem that must be approached from the top. When the castle walls continue to be regularly breached, it's not time to continue to build higher walls and deeper moats. A redesigned company-wide approach that includes all departments, partners, suppliers, and attention to insider threat is long overdue.

Become a Resource

To become an effective resource against today's threats, it's important to understand the true threat behind data breaches, the scale and motivations involved. This is only accomplished through active, on-going intelligence and counterintelligence.

There are two classes of threats: nation-state and "privateers." Each type is very different in intent, approach, means, and scope. Nation-state attacks are government-based, well planned, massive, decades long, and designed to steal innovation and trade secrets on a grand scale. This eliminates the requirements of time and funding for research and development. Secrecy and plausible deniability are the primary components of nation-state threats. Research and experience proves that 99% of nation-state breaches go unreported or, worse, undetected.[6]

The second class of threat is the "privateer." This is usually a lone wolf or small group of hackers who are opportunistic and have the intent to steal private data for immediate sale on the DarkNet. These breaches typically involve personally identifiable information (PII). In a recent experiment by Bitglass, "stolen" data was viewed more than1000 times and downloaded 47 times by people in 22 counties on five continents.[7] BLACKOPS Partners intelligence also shows stolen data is typically parsed and resold an average of five times. For example, this equates to 10 million stolen records having the effective damage of 50 million. Most of these breaches are exposed when they are listed on the DarkNet for sale and reported as required by regulators.

You Don't Know What You Don't Know

To add real value for CEOs and Boards, an effective cybersecurity strategy must incorporate a 180 degree departure from our expired defensive strategy. The cybersecurity industry has traditionally been built upon a collection of software and hardware products requiring patches and updates. Many of the products currently in use have become obsolete in this fast-moving threat environment. Defending the "castle wall" became obsolete years ago. The old way of thinking must make way for a new thought process. Changing nothing risks everything.

To effectively defend against a nation-state, privateer hacker, or insider threat, we must begin to think like our adversary on a fluid security model. It is this core transformation that truly yields the breakthrough protection companies desperately require today. This is also the point where we become valuable to the CEO and board. Mike Tyson said it best: "Everyone has a plan 'till they get punched in the mouth."

Understand the Board's Role

In their role of active oversight, the board does not need to know specific technological details. However, they require enough detail to review and make effective decisions on where to place focus, resources, and funding. Data breaches are a new and increasingly massive business risk that CEOs and boards must learn to manage effectively.

Speak Their Language

CEOs and boards rarely come from cybersecurity or technology backgrounds. They are focused on business

risk and the business impact of data breaches, their total cost over time, potential revenue hit, and damage to the company's reputation over time.

Provide context and comparisons in terms of data breach specifics by listing and quantifying the business risks the breached companies incurred. Include a cost/benefit analysis in support of your recommendations to manage and reduce business risk.

Answer Key Questions

Now that data breaches have become the norm, directors must handle the cybersecurity curve quickly. CEOs and boards have little training in cybersecurity but have the fiduciary responsibility to actively oversee it. In many cases, they don't know the correct questions to ask. The following questions are an excellent opportunity to begin a next-level relationship with your board. Be sure you have solid answers to each question before you sit down.

1. Where is our sensitive data stored?
2. Who has access to it? How is access managed?
3. Where is our sensitive data going?
4. What can we do to limit it?
5. How do we limit damage to our reputation?
6. How do we protect our reputation?

Get Them Involved

The most effective way to increase your CEO and board's cybersecurity literacy is to schedule them "hands-on" with a cyber breach exercise facilitated by a highly experienced third party. Include all key executives and document the process. Repeat it twice per year or annually, at a minimum. When directors walk through the process, it becomes enlightening for everyone involved. Each participant gains understanding and appreciation for each other's role in the exercise. A shared breach exercise with officers and directors is the cornerstone to next-level cybersecurity literacy and a productive relationship going forward.

Sources

1 Fisher, Daniel: "If 2014 Was The Year Of The Data Breach, Brace For More." Forbes.com, January 2015.
<http://www.forbes.com/sites/danielfisher/2015/01/02/if-2014-was-the-year-of-the-data-breach-brace-for-more/>

2 Storm, Darlene: "FireEye suspects FIN4 hackers are Americans after insider info to game stock market." Computerworld.com, December 2014.
<http://www.computerworld.com/article/2853697/fireeye-suspects-fin4-hackers-are-americans-after-insider-info-to-game-stock-market.html>

3 Viebeck, Elise: "FBI: Data breaches 'increasing substantially'." TheHill.com, May 2015.
<http://thehill.com/policy/cybersecurity/242110-fbi-official-data-breaches-increasing-substantially>

4 Reisinger, Sue: "Data Breaches on Track to Cost Companies $2.1 Trillion." Corpcounsel.com, May 2015.
<http://www.corpcounsel.com/id=1202726318756/Data-Breaches-on-Track-to-Cost-Companies-3621-Trillion?slreturn=20150515184638>

5 "Cybersecurity Lessons for the C Suite." Chiefexecutive.net, May 2015.
<http://chiefexecutive.net/cybersecurity-lessons-for-the-c-suite/>

6 BLACKOPS Partners intelligence

7 "Experiment Shows Speed at Which Stolen Data Travels." Wallstreetjournal.com, April 2015.
<http://blogs.wsj.com/riskandcompliance/2015/04/15/experiment-shows-speed-at-which-stolen-data-travels/>

About the Authors:

T. Casey Fleming *serves as Chairman and Chief Executive Officer of BLACKOPS Partners Corporation, the leading management advisors consisting of America's elite executive thought leaders from intelligence, technology, federal law enforcement, information security, and management consulting. Mr. Fleming is a leading expert in risk reduction and the advanced protection of innovation, trade secrets, and competitive advantage for Fortune 500 companies, U.S. government agencies, universities, and research facilities. Mr. Fleming is an innovative information security and management consulting executive who directed organizations for Good Technology, Deloitte Consulting, and was a founding executive of IBM's Cyber division. Mr. Fleming earned his Bachelor of Science from Texas A&M University.*

Anthony M. Chapa *serves on the Board of Directors for BLACKOPS Partners Corporation. Mr. Chapa is the CEO of Chapa Concepts, which provides threat and technology assessment for leading advanced technology and public sector organizations. In addition, Chapa Concepts provides strategy and operational support to biometric access, security technology, and communication firms. Mr. Chapa retired from the United States Secret Service (USSS), Department of Homeland Security after a highly successful career, including as Assistant Director at USSS Headquarters and Deputy Assistant Director and Chief Technology Officer responsible for the Technical Security Division. Mr. Chapa also served as the Special Agent in Charge of the Los Angeles field office including leadership over the nation's premier USSS Electronic Crimes Task Force (ECTF). Mr. Chapa earned his Bachelor of Arts and Master of Arts in Political Science from St. Mary's University.*

BLACKOPS PARTNERS