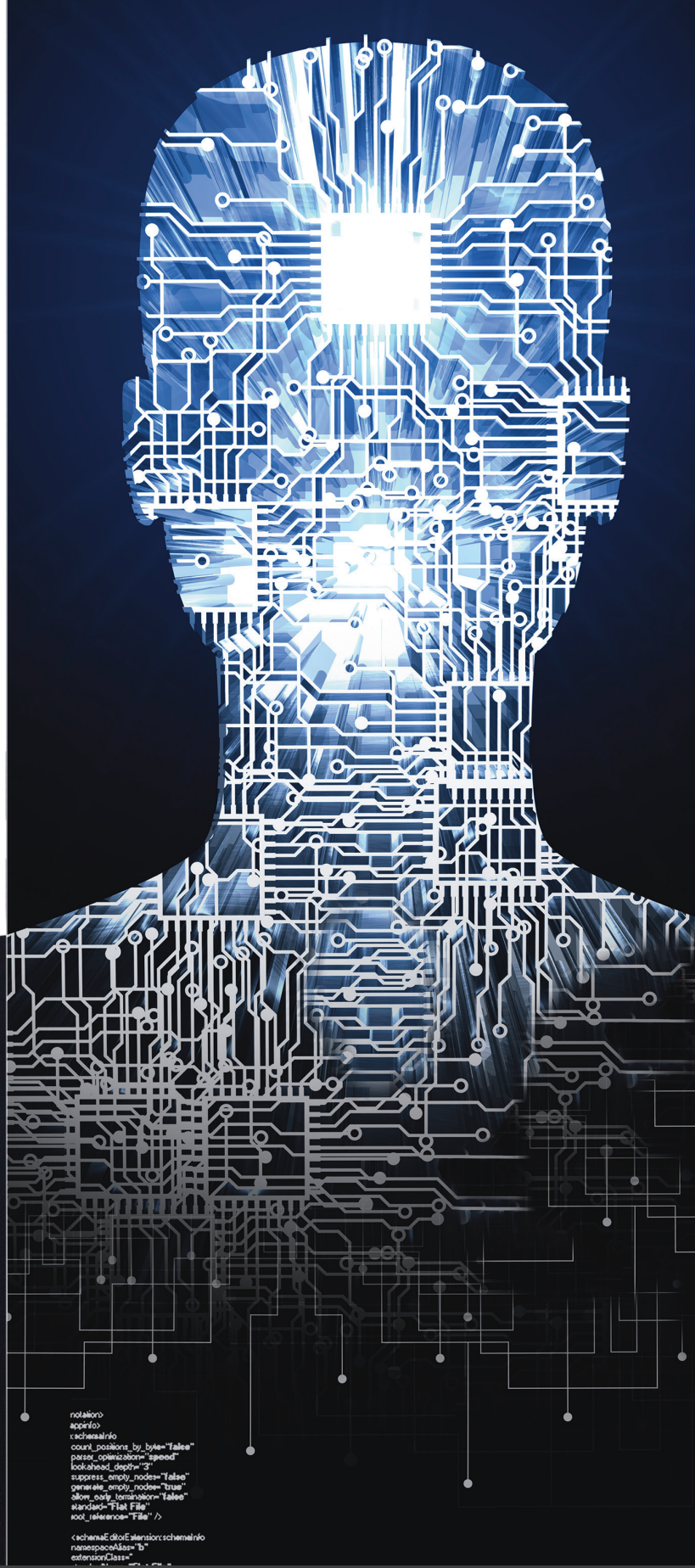
C-SUITE

An Equilar publication
Issue 26, Winter 2018



The AI Evolution

Why all boards should be thinking about artificial intelligence in 2018

A roller coaster year for corporate governance

Protecting the board against shareholder scrutiny

Hot-button boardroom issues for 2018

Creating diverse board committees

Interviews with Betsy Atkins, CEO and Founder of Baja Corporation and multi-boarded director, and James Lam, board member at E*TRADE Financial

EQUILAR

Five Critical Cybersecurity Trends (and More) for 2018

An interview with James Lam, board member at E*TRADE Financial

James C. Lam is the President of James Lam & Associates and a Director of E*TRADE Financial, where he chairs the risk oversight committee and serves on the audit committee. He previously served as President of ERisk, partner of Oliver Wyman, Chief Risk Officer of Fidelity Investments, and Chief Risk Officer of GE Capital Markets Services. Lam was named to the NACD Directorship 100, Directors & Boards Diversity Directors to Watch, Treasury & Risk 100 Most Influential People in Finance, and GARP Inaugural Risk Manager of the Year. He is the author of multiple best-selling books published by Wiley.

High-profile data breaches continue to hit large corporations. Yahoo, Equifax and Uber are just three examples in the past year that have kept corporate cybersecurity in the spotlight, but boards recognize that large or small, there is imminent risk for their companies. The question all boards have to answer is how can they protect themselves and ask the right questions of management? Building cybersecurity framework into their enterprise risk management is critical, and knowing how to stay on top of the latest threats and trends is one of the most important duties a board has today. *C-Suite* had the opportunity to speak with James Lam, President of James Lam & Associates and a Director of E*TRADE Financial, where he chairs the risk oversight committee and serves on the audit committee, to discuss the cyber landscape, how the board should act and react, as well as what to expect in the near- and mid-term.

C-Suite: How would you evaluate the current approach to cybersecurity at the board level? What elements are directors missing as they evaluate cyber risk, even if they've "checked the boxes" to have the right pieces in place?

James Lam: Corporate directors are taking cybersecurity very seriously. A few years ago boards might discuss cybersecurity once or twice a year. Today it is likely to be discussed at every board or committee meeting. Boards are clearly paying more attention and spending more time on cybersecurity issues. In the recent board surveys that I have seen, cybersecurity is usually a top-three or top-five concern for directors.

There is a "check-the-box" element when it comes to regulatory compliance, such as SEC disclosure requirements for public companies, applicable industry-specific and state-level regulations, and the General Data Protection Regulation (GDPR) for companies doing business in the E.U. However, regulatory standards only provide a baseline for cybersecurity preparedness. Companies should go beyond regulatory requirements and establish a security program that is appropriate for their industry, size and complexity. Moreover, as corporate directors we need to address cybersecurity as a business and risk issue, and not just a security or compliance concern.

Directors need to be confident that a good chief information security officer (CISO) is in place, that the right level of spending and resources are allocated to the appropriate controls, and that the company is properly secured against a cyberattack. But we also need to consider cyber risk in the broader context of other enterprise risks, including strategic, operational and financial risks. Additionally, we must balance cyber risk with the opportunity side of doing business in the digital economy. To compete effectively, we need to disrupt our own business models, enhance the customer experience and introduce new product innovations. We can't be timid about technology because we have security concerns.

How can companies better balance digital opportunities and cyber risks? What should directors ask for in evaluating risk/return trade-offs?

Lam: At a fundamental level, the processes for strategy development, execution and performance monitoring must be integrated with the processes for risk identification, risk assessment and risk management. If these processes are disjointed, then it is impossible to understand risk/return economics. It would be silly to have a revenue statement separate from an expense statement and not put them together to measure net profit. That is what happens when strategy is not integrated with risk management.

Ultimately, our digital strategies are meant to increase long-term profitability and enterprise value. We would measure that in economic terms. But what is the cost of risk, including technology, operational and cyber risks? We should likewise measure that in economic terms. By doing so, we can compute the risk-adjusted ROI of digital strategies.

Moreover, a value-based approach to cybersecurity can inform the board with respect to the trends in the company's cyber risk profile, the cost-effectiveness of existing and proposed controls, and whether the company should transfer some of its risk through cyber insurance.

> AI and machine learning will be a blessing and a curse for cybersecurity. I would add data analytics and quantum computing to that grouping. As with any toolset, it can be used for good or evil.

For what other reasons is it so critical that companies address this now, and to what should the board pay special attention?

Lam: A heightened sense of urgency is essential. In many respects it is a race against time. On the opportunity side, we need to be faster, cheaper and more innovative than our existing and emerging competitors. On the security side, we need to be much faster in adopting layered defenses and proactive strategies as cybercriminals gain access to sophisticated attack weapons that were once available only to nation-states.

It is also a race against time in the event of a breach. It has been reported that 80% of large U.S. companies have been breached, so we can't put too much reliance on preventative controls. What is the time to detect, the time to mitigate and the time to recover? To the extent we can compress these time dimensions we will reduce potential data, financial and reputational loss. For example, the average time to detect a breach, or adversary dwell time, is over three months. We all have to do much better.

The board should focus on people and culture when it comes to cybersecurity. In most circumstances, people represent the weakest link and one of the first points of vulnerability that hackers target. Therefore, human behavior and corporate culture can have more impact on cyber preparedness than security policies, systems and processes combined. As such, directors should pay special attention to the cybersecurity awareness and training programs, as well as behavioral analytics of employees and contractors.

Do widely established industry "best practices" make it easier for hackers to stay ahead of the current market trends (i.e., couldn't they just find another way if companies protect against the current threats)? What are the challenges and strategies to consider in addition to addressing what is already known?

Lam: As cybercriminals cooperate with nation-states, and as these actors increasingly use blended strategies to attack our digital and physical infrastructure, we will

> "The board should focus on people and culture when it comes to cybersecurity."

always face "known unknowns" and "unknown unknowns." However, zero-day attacks and new attack patterns are not common.

Companies are better off paying more attention to "known knowns" or basic hygiene. These basic hygiene areas include strong passwords, multi-factor authentication, minimum privileged access, timely patching, and regular phishing and penetration testing. The overwhelming portion of cyber breaches come from cybercriminals exploiting the lack of these basic controls. Companies should also minimize the surface area for attacks by securing their "crown jewels," and segmenting their databases and networks. On a regular basis, directors should ask tough questions and demand ongoing reporting of these known risks.

Beyond basic hygiene, companies should establish performance feedback loops that will systematically capture the variances between actual risks vs. expected risks. For example, if the company sees new attack weapons and patterns that were not on its radar screen, then it must make the necessary changes to its cybersecurity program. The purpose of a performance feedback loop is to facilitate continuous improvement by minimizing the variance between actual risks and expected risks. In other words, we want to implement self-correcting measures that will rapidly move threats from the "unknowns" to the "knowns."

In what ways will the introduction of AI and machine learning aid cybersecurity practices? To what degree will these technological advancements aid attackers, and how does that complicate the risk evaluation process for boards?

Lam: Directors should stay on top of these key technological developments. AI and machine learning will be a blessing and a curse for cybersecurity. I would add data analytics and quantum computing to that grouping. As with any toolset, it can be used for good or evil. Sadly, the cybercriminals are probably having such easy success in exploiting basic hygiene weaknesses that it has not been necessary for them to invest in these tools.

At a pace that is increasing exponentially, we are creating and storing a vast amount of data through social media platforms and the internet of things. These advanced tools—data analytics, quantum computing, machine learning and AI—will help turn that data into actionable intelligence. For cybersecurity, these tools can extract a vast amount of internal and external data, flag network vulnerabilities, and predict the likelihood of breach far better and faster than current techniques. As cyber defense gets smarter, so will the offense. This is another technological arms race where defensive and offensive actors co-evolve in developing and implementing more and more advanced systems.

What can companies learn from others' breaches, both in terms of protecting against them, and then how to address breaches if they are hit? (Equifax, Yahoo and Uber come to mind on the latter.)

> "When I was growing up, one of the key lessons that my father taught me is that 'a smart man learns from his own mistakes, a wise man learns from the mistakes of others and a fool never learns.'"

Lam: When I was growing up, one of the key lessons that my father taught me is that "a smart man learns from his own mistakes, a wise man learns from the mistakes of others and a fool never learns." This is a lesson that should be applied by all risk professionals. In enterprise risk management (ERM), the loss-event database is a widely used technique. Such a database would systematically capture all material losses, risk events and even near misses. The ERM function would establish a monthly process to review these losses and events, identify root causes, and implement new controls. Companies have reported significant reductions in operational losses based on this simple technique.

Whenever there is a significant breach at another company the board should always ask: What happened and what are the underlying root causes? Do we have similar vulnerabilities, and could that happen here? What are the lessons we should learn with respect to our cybersecurity program?

One of the key issues in the major breaches is how timely and forthright the company is in communicating to its stakeholders, including customers, law enforcement, regulators, shareholders and the general public. The board should make sure that an updated and tested crisis communication plan is in place in case of a breach.

Cybercriminals will launch blended attacks that are increasingly more sophisticated, audacious and consequential.

How do cybersecurity frameworks and guidelines play into directors' evaluation of cyber risk? What don't those address that directors want to know?

Lam: Directors should get an independent assessment of the company's current cybersecurity program relative to the standards established in cybersecurity maturity frameworks such as NIST and ISO 27001. Based on this assessment, action plans should be developed to close any significant gaps. While this exercise is necessary, it is also insufficient. A more mature program doesn't always equate to a more effective program.

The average CISO at a large company has more than four dozen security vendor relationships. Maturity models always produce an answer that says more—add people, add systems and add processes. But is more always better? Directors are rightfully concerned about program effectiveness and overall preparedness (output) and not just program maturity and control components (input).

These frameworks do not fully meet the needs of the board. Consider the five components of NIST: protect, identify, detect, respond and recover. These are the processes that the CIO or CISO must develop and implement. Directors are also concerned with key issues that are not addressed by NIST, including alignment with the overall business strategy, cybersecurity risk policy and risk appetite, cyber risk quantification, and overall cybersecurity program effectiveness.

How do you see cybersecurity evolving in the coming years?

Lam: Here are the five key trends that I would look for in 2018 and beyond:

1. Cybercriminals will launch blended attacks that are increasingly more sophisticated, audacious and consequential. At the end of 2015, the first known cyberattack that caused widespread blackouts was reported in the Ukraine. Meanwhile, ransomware damages have soared from $325 million in 2015 to $5 billion in 2017. We will likely see more state-sponsored attacks, some with the help of criminal enterprises. There will also be more cyber events that target both digital and physical infrastructure.
2. Corporate executives and directors will face new regulations with more stringent standards for governance, privacy, security and disclosure. These new regulations will add to the regulatory complexity and compliance costs associated with existing requirements. It doesn't help that regulatory standards are often inconsistent, and sometimes even conflicting, across regulatory agencies, states and countries.
3. In terms of risk management practice, cybersecurity will be more integrated into ERM. By leveraging ERM methodologies—such as the three lines of defense model, risk appetite statement, loss/event database, risk-control self-assessments and key risk indicators—companies will better monitor their overall risk profiles and manage the interdependencies across risks. An example would be the interdependences between cyber risk and third-party vendor oversight, operational risk management and business contingency planning.
4. Directors will demand much better cyber risk reporting from their CISOs. The 2017-2018 NACD Public Company Governance Survey found that 22% percent of directors expressed dissatisfaction with the quality of cyber risk information. That number should be zero. It is management's responsibility to produce a board-level cyber risk report that is clear and understandable. Directors will receive cyber risk reports that include expert commentary from the CISO, trends in the external threat environment, cyber risk indicators against risk tolerance levels, independent security ratings benchmarked against peers, and performance metrics of key controls and the overall cybersecurity program.
5. Advanced technologies and tools will be developed to help companies measure, monitor and manage their cyber risk profile. We have discussed how advanced tools—data analytics, quantum computing, machine learning and AI—will produce actionable intelligence and enhance our cyber defense. Additionally, cyber risk quantification models will be developed and implemented to measure value-at-risk (VaR) on an ongoing basis. VaR models have been used for many years to quantify market risk, credit risk and, more recently, operational risk. Cyber VaR models will help companies monitor their cyber risk profiles, evaluate the cost effectiveness of security controls and determine the economic value of cyber insurance. CS