Securing Confidence in a Company's Cyber Efforts

By Jeff Ward, CPA and Don Sheehy, CPA

Jeff Ward is the National Managing Partner of BDO USA's Third Party Attestation practice. He has over 30 years of IT audit-related experience and focuses primarily on cybersecurity, public key infrastructure and encryption. He has been active on various task force standards for both CPA Canada and the American Institute of Certified Public Accountants, and is the inaugural Chairman of the Missouri CPA Society's Transformation Task Force.

Don is a retired BIG 4 partner who consults in Canada and the United States in PKI Assurance and Third Party SOC (and related) reporting, having spent more than 20 years in delivering such services. He has been involved in a number of CPA Canada and AICPA task forces dealing with SOC reporting, Privacy, Cybersecurity and PKI. He is currently vice-chair of the CPA Canada PKI Assurance Task Force.

The World in 2020

The significant business disruption that has occurred during the coronavirus, or Covid 19, crisis will have a major impact on how boards of directors around the globe think over the long term about working remotely and its impact on privacy and cybersecurity.

As the pandemic creates economic uncertainty, some directors are attending frequent virtual meetings to discuss their concerns with management. Hackers are capitalizing on coronavirus fear with phishing campaigns and are seeking out vulnerable home networks and video-conferencing applications. Risk and audit committees, in particular, are asking executives to spell out cybersecurity measures that their company is taking to protect data while employees work remotely, and to develop contingency plans to address such risks. This is an emerging trend that will only continue within the ranks of those charged with governance.

"Boards are getting in deeper," says Howard Brownstein, president of Philadelphia-based restructuring firm Brownstein Corp. "We're not going to wait for our next quarterly meeting." Brownstein said his boards are holding special sessions or extra committee meetings to cover these issues. He serves on the boards of manufacturer P&F Industries Inc., education and health-care nonprofit Merakey and a chapter of the National Association of Corporate Directors.

Boards are balancing these concerns with longer-term issues about maintaining customers and operations, adds Andrea Bonime-Blanc, chief executive of GEC Risk Advisory LLC, a New York-

based firm that advises boards and executives about cybersecurity and risk management. "It's a perfect storm of crisis and business continuity challenges."

Bonime-Blanc recommends that directors ask management for specific details about how their company backs up data to make sure that it remains accessible during a crisis, how critical data is protected and whether suppliers are secure. If boards don't already have baseline reporting about these issues from before the pandemic, it will be difficult to catch up and assess how the company is faring, she says.

According to Lorenzo Fantini, a Milan-based managing director at Boston Consulting Group, companies are struggling to understand potential long-term effects of the pandemic because it isn't clear if government restrictions will remain for the next few weeks or months or potentially into next year. Directors can help management plan for different levels of virus infection and government restrictions, he adds. Concerns will continue for the foreseeable future as the World Health Organizations warns of a second wave of the novel coronavirus this fall.

Hackers are capitalizing on coronavirus fear with phishing campaigns and are seeking out vulnerable home networks and video-conferencing applications.

The current pandemic has put traditional supply chains to the test, causing companies to rethink their go-forward strategy. Fantini co-authored a Boston Consulting Group report published last month describing a hypothetical example of an automotive manufacturer that relies on a component supplier in a location highly affected by the novel coronavirus. The report advised the manufacturer to plan for potentially shutting its factory and to discuss contingencies with its board.

Because of product shortages that companies are experiencing during the pandemic, board members may become more willing to share data with governments, suppliers and other companies because doing so could make supply chains more resilient, says Michael Hilb, a professor of corporate governance at the University of Fribourg in Switzerland.

Product shortages rippled through supply chains after governments ordered nonessential businesses to shut down, explains Hilb, who sits on the boards of Swiss industrial manufacturer Klingelnberg Ltd. and the nonprofit Board Foundation. Directors have "taken a very conservative approach, particularly in Europe, toward any kind of data sharing. That attitude has changed or will change," he notes.

Meanwhile – Cyber Security Attacks Are Rising

Somewhere lost in the news is that cybersecurity attacks are still an ongoing battle for companies. As we know, cybersecurity attacks continue to be on the rise and likely will be for the foreseeable future. In fact, according to Vailmail's 2018 Global Information Security Survey, more than 6.4 billion fake emails are sent everyday by nation-state cyber-attack groups, criminal cyber-attack groups and hackers worldwide. This results in the theft of over two billion private identities and $3.5 billion in cyber damages daily. To combat the ever-growing global cyber attacks in both the public and private sectors, the cybersecurity marketplace has expanded to $100 billion in annual purchases of software, hardware and related cybersecurity professional services, with a 12% Compounded Annual Growth Rate (CAGR), as reported by the Gartner Group.

When assessing confidence and evaluating a company's cybersecurity efforts, stakeholders are analyzing, to some extent, steps taken by industry peers. This means that, at any given time, risk may be measured for your peers' businesses based on what you are doing, and vice versa. This is called the "contagion" effect, according to a recent study conducted at North Carolina State University, which reveals that, when one company experiences a cybersecurity breach, other companies in the same field can also become less attractive to investors. Companies that

are forthcoming about their cybersecurity risk management efforts, however, fare significantly better than those that wait until it's required.

Future Risks and Trends

So where is all of this headed? Despite the growing investment in cybersecurity, the public and private sectors are not keeping up with needed training, policy and controls – we now see an estimated $4.2 trillion in annual global fraud, theft and data breach damages caused by cyber attackers; this is predicted to exceed $6 trillion in cyberattack-related damages by 2021.

> No single product or service can provide a magic solution to this multifaceted, ever-evolving and highly complex set of global information security challenges.

Forester Research estimates that fewer than 2% of all information technology professionals globally are educated, trained, certified and actively working as cybersecurity professionals. Clearly, government organizations, publicly traded companies and privately owned companies need to take the threat of cyber attacks more seriously by investing more resources in creating an effective cyber defense. Realizing that 40% or more of cyber vulnerabilities are directly linked to employee behaviour, per the Gartner Group's latest studies, it is vital that organizations focus more on their employees via cybersecurity awareness, education, training and use of simulations to create a stronger human firewall to protect their vital digital assets.

As companies deal with the current and future risks and trends beyond 2020, it is important to consider the following:

- *Continued Global Shortage of Cybersecurity Talent*. There continues to be an on-going under-investment in cybersecurity education, training and certification programs at the undergraduate, graduate and continuing education levels. Combined with the incredible increase in cyber attacks globally, this has resulted in a significant shortage of cybersecurity professionals and related data scientists required to meet the increased cybersecurity demands worldwide.

- *Rise of Insider Threat Cyber-Attacks*. As organizations improve their overall integrated cyber defense via enhanced investments in cybersecurity training, encryption, multi-factor authentication, zero trust architecture, advanced data analytics, continuous diagnostics, monitoring, detection and incident response, cyber-attackers will seek to by-pass all of the security measures by bribing employees who have restricted access to valuable intellectual property and key data assets in order to steal the data.

- *Expansion of IoT Cyber-Attacks*. According to Symantec, the number of Internet of Things (IoT) connected devices is estimated to rapidly increase from 10 billion devices in 2017 to

more than 26 billion devices by the end of 2020. With the tremendous increase in the number of such devices, it is anticipated that there will be a dramatic increase in the number of cyber-attacks on IoT connected devices, especially medical devices.

- *Growth of Distributed Denial of Service (DDoS) Cyber-Attacks*. The significant success of DDoS cyber-attacks in the past years suggests that these cyber-attacks will continue to increase worldwide, especially in the retail, consumer products and critical infrastructure industries, where they have experienced the greatest impact.

- *Increase in Cyber-Impersonation Attacks and Business Email Compromise (BEC) Attacks*. During the past 18 months, the use of socially-engineered cyber impersonation attacks and BEC attacks have grown exponentially in both number and sophistication, specifically targeting senior executives in both government agencies and the private sector to re-direct payments to cyber-attackers, usually intended for business partners or suppliers.

- *Exploitation of Cyber Weakest Link Attacks on Supply-Chains*. With the success of cyber-attacks on global supply-chains across numerous industries, including oil, gas, energy, defense, aerospace, healthcare, manufacturing, retail and consumer products, we can expect an increase of cyber-attacks targeting the most vulnerable organizations in supply-chain networks, which are usually small business vendors/third-party suppliers, aimed at gaining access to the intellectual property of larger organizations.

- *Lack of Empowerment in CISO Role*. Too many organizations have not adequately empowered and supported their Chief Information Security Officer (CISO) with the funding, resources and senior executive commitment to ensure an appropriate level of cyber defense. Most organizations continue to care far more about their network data capacity, ease of data access and software applications than the protection of the data assets and the resilience of the information system in facing damaging cyber attacks.

- *Increasingly Complex Cybersecurity and Data Privacy Regulatory Landscape*. As companies all strive to protect themselves and their personal identifiable information from the growing number of cyber fraud cases and cyber data breaches, the number and complexity of new cybersecurity and data privacy laws, regulations, standards and contractual requirements are rapidly increasing. This results in the rise of potential civil and criminal penalties for non-compliance, including: European Union (EU) General Data Privacy Regulation (GDPR), ISO 27001 Information Security Standard, National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework (RMF), the Payment Card Industry (PCI) Data Security Standard (DSS), the New York Department of Financial Services (NYDFS)'s cybersecurity requirements for financial institutions and the California Consumer Privacy Act (CCPA), just to name a few.

To deal with the increasing risks, companies are exploring the use of new cyber strategies including:

- *Growth of Zero Trust Cyber Data Architecture*. Increasingly, organizations are adopting the Zero Trust software architecture approach to thwart the damages of cyber-attacks. The Zero Trust Architecture method is designed to create micro-perimeters within information systems to increase data segmentation and establish micro-firewalls within the network to reduce the ease of lateral movements by cyber attackers within an information system once an intrusion has occurred.

- *Explosion in the Use of Machine Learning or Artificial Intelligence to Combat Cyber Attacks*. Organizations worldwide are exploring numerous use cases to implement machine learning and/or artificial intelligence to enhance proactive cyber defense tactics and optimize cyber-attack monitoring, intrusion detection and incident response capabilities.

The current pandemic has put traditional supply chains to the test, causing companies to rethink their go-forward strategy.

Effective Cyber Program Development

Cyber awareness is an entity-wide issue; unfortunately, responsibility for cyber-related efforts oftentimes falls on IT. We often see board members – who are typically most visible to investors – with little to no insight into their company's cyber-related programs. According to BDO's recent survey of board directors, 39% said they were only somewhat or not at all familiar with their organization's data breach response plan. Another 37% said they were moderately familiar. Meanwhile, when asked if their company had cyber risk requirements that third-party vendors must comply with, 27% answered that they were not sure.

Keeping abreast of cybersecurity risk is a daunting task, so no wonder that the survey's results did not yield more favorable results pertaining to knowledge in this area on the part of those charged with governance. After all, the cybersecurity marketplace has rapidly grown to a $100 billion industry, offering a wide range of cybersecurity hardware, software and professional services. There are now an incredible number of companies offering cybersecurity technologies, products and services, often claiming to have the solution to many of your cybersecurity needs. Unfortunately, no single product or service can provide a magic solution to this multifaceted, ever-evolving and highly complex set of global information security challenges.

Thus, many C-suite executives are trying to make the right investment decisions, but often they are not well informed about the cybersecurity threats facing their organizations and all the potential cybersecurity liabilities. Rather than investing valuable resources in protecting specific types of high-value data, a threat-based approach to cybersecurity identifies the vulnerabilities that a cyber-attack would likely try to exploit, and outlines measures to secure those vulnerabilities.

Based on one of the authors' professional experience as BDO's US National Managing Partner Third Party Attestation, when board members tell stakeholders what their cyber risk looks like, they need to be able to answer the question, "How do you know?" Just as boards receive internal financial statements and are well-versed in how they're tracking on sales, accounts receivable and where their business is falling short, they should have the same level of insight into their cybersecurity function.

When a company falls victim to a cyber breach, the most common knee-jerk reaction is to develop an incident response plan that tackles the vulnerability at hand. A software patch, for instance, is a quick fix, but it fails to address the broader picture. It's critical to have a comprehensive cybersecurity risk management program in place that aligns with overall business strategies. It should cover asset identification all the way through to reporting and remediation in the event of a breach. This is not to suggest that a cybersecurity risk management should only focus on financial systems, nor is it just an IT issue.

> More than 6.4 billion fake emails are sent everyday by nation-state cyber-attack groups, criminal cyber-attack groups and hackers worldwide.

So How Do Breaches Occur?

How do breaches go undetected for prolonged period of times? While there are many reasons companies fall victim to attack, there are some common pitfalls that organizations have to avoid, such as:

- Selecting an unqualified individual to serve as your organization's IT Security Director or Chief Information Security Officer.
- Underinvesting in cybersecurity education and training for the entire organization from the top to the bottom.
- Assuming your Cyber Liability Insurance Policy will fully cover the damages of a cyber data breach.
- Failing to conduct continuous cybersecurity monitoring and intrusion detection of email systems, networks, software applications and endpoints.
- Failing to conduct regular computer software vulnerability scanning and penetration testing.
- Waiting until after a cyber data breach to find, read and test your organization's cyber Incident Response Plan.
- Failing to develop a Business Continuity Plan and Disaster Recovery Plan.
- Expecting compliance with a Cybersecurity Risk Management Framework (i.e., ISO 27001, NIST SP 800- 171, PCI-DSS, HITRUST/CSF, etc.) to prevent a cyber data breach.
- Postponing implementation of a timely software patch management program.

- Assuming your suppliers/vendors have adequate cybersecurity.

Assessing a Cyber Risk Management Program

The C-suite worldwide is increasingly concerned about the growing risk of a massive cyber data breach, like those encountered by Capital One, Facebook, Equifax and numerous government agencies. Thus, C-level executives within all organizations need to understand the value of the information assets they possess, the cybersecurity and privacy related risks, and then factor the benefits of cybersecurity investments and risk variables into their respective business equation.

While companies have historically faced challenges in communicating with investors and other stakeholders on their cybersecurity risk management programs, CPA Canada and the American Institute of Certified Publc Accountants have created a service, SOC for Cybersecurity, which provides description criteria for entities to use when assessing their cybersecurity programs. Control criteria in place (such as NIST, ISO, Trust Services Criteria) are then evaluated to ensure the appropriate controls for financial, operational and administrative areas are in place. The SOC for Cybersecurity framework can be used internally for an organization and can also be subjected to an independent third party conducted by a qualified audit firm. Although following these guidelines for cyber reporting is a good first step, you're lent additional credence when you have a third party verify that you are, in fact, meeting the guidelines.

Some companies are hesitant to go down the path of auditing their cyber efforts out of fear that it will uncover weaknesses and shine a spotlight on non-compliance issues. But the fact is, transparency and proactivity can help offset negative publicity and regulatory scrutiny in the aftermath of a breach.

Whether your cyber risk is under examination due to a data breach within your organization or a peer's, presenting a SOC for Cyber assessment could assuage stakeholder concerns. It proves you have met CPA Canada and the AICPA's voluntary reporting guidelines and are proactive about protecting your business' and customers' critical data assets.

All-Inclusive Strategies Work Best

Simply put, it is vital that C-suite executives adopt a threat-based cybersecurity strategy to understand the cyber threats they are facing, and then make the right investments to mitigate identified vulnerabilities, thereby reducing their cyber liability while also maximizing resources. Proper cybersecurity strategies encompass the entity as a whole, need to have cross representation among the various departments of the firm, need board support and need to be continuously monitored and updated. After all, cybersecurity is the responsibility of everyone in the organization.

OIO