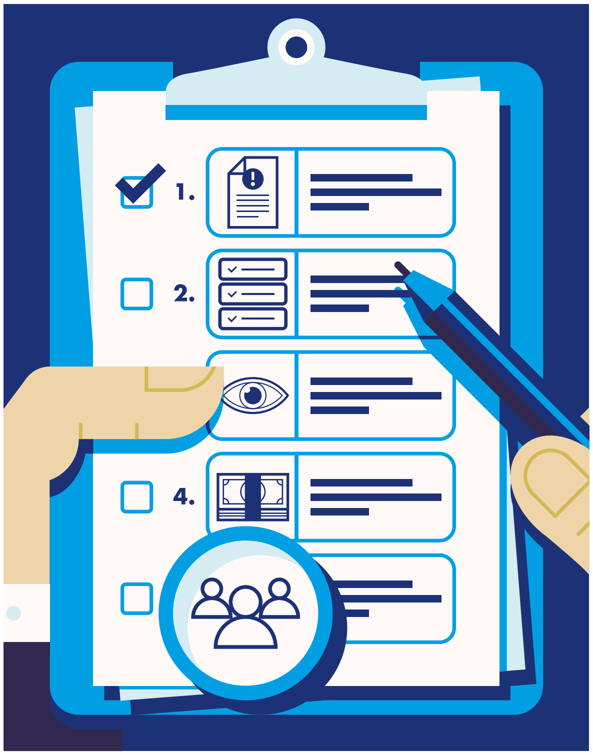
BIG ASK: WHAT DON'T YOU KNOW ABOUT CYBERSECURITY?

**Boards need the best information.
For that, they need to know the right questions,
say Brunswick's GEORGE LITTLE and SOFIA MATA-LECLERC**



IN THE PAST THREE YEARS, a growing number of high-profile attacks in a broad range of sectors, including financial and healthcare, have exposed the personal records of millions and propelled cybersecurity to the top of the corporate board agenda. The concern is real. A recent study by IBM found that 94 percent of C-suite executives believe it is probable their companies will experience a significant cybersecurity incident in the next two years.

A breach can result in a loss of data, intellectual property and customer trust. In more severe cases, a breach can cripple a company's ability to operate. Aftershocks include reputational damage, resignations, fines, regulatory action, lost business and class action lawsuits. The average cost of a data breach has risen 23 percent since 2014, according to the Ponemon Institute, a data security research organization.

Recent Brunswick Insight research finds 74 percent of board directors agree that it is important to understand the cyber risks. Yet Gavin Patterson, CEO of telecommunications group BT, told delegates at the World Economic Forum in Davos that most boards still lack the experience to handle such challenges.

"The risk is changing in its nature and is becoming more sophisticated," he said. "While I think there is a recognition at board level now, I'm not always convinced when I talk to other CEOs that there is a high technical understanding."

Meanwhile, the stakes are getting personal. Data-breach related lawsuits have been filed against the boards of Target, Wyndham Worldwide and Home Depot. Plaintiffs claim that board members failed to fulfill their fiduciary duty to protect customers' information.

Cybersecurity is a complicated issue that can arise out of any business decision, not just those involving IT. While board directors aren't expected to be experts, they do need an advanced understanding of the risks facing the company and a familiarity with the procedures in place to handle a cyber attack. Boards should seek outside cyber expertise, says Holly Gregory, a Partner at corporate law firm Sidley Austin. But in the end, the responsibility for the effects on the company rests with the board.

"Ultimately, the 'business judgment rule' should apply to any decisions regarding oversight of cybersecurity issues," Gregory says. In other words, "directors should abide by the core standards of care, loyalty and good faith that apply to board actions generally."

Regular dialogue about a company's cyber risk management helps ensure this remains a priority for leadership. The form and frequency of board briefings will vary according to the company's size, type of data collected and the nature of the cybersecurity issues it faces.

Each board must decide for itself how to structure that conversation among its members. Some may choose to appoint a cybersecurity director or create a specialized committee.

No matter how it is handled, an effective cybersecurity strategy requires more than just one decision or discussion. Boards must make a commitment to regularly review and update their understanding of the risks.

They may not need to be experts, but they must be informed. For that, they need to know what to ask.

GEORGE LITTLE is a Partner in Brunswick's Washington, DC office, specializing in crisis, cybersecurity, reputational and public affairs. **SOFIA MATA-LECLERC** is a Director in San Francisco, specializing in crisis, cybersecurity and corporate reputation.

Five questions every board should ask

1. What procedures do you have in place to manage a breach?

An ideal response will demonstrate that the company has thought through multiple scenarios. Plans for handling a breach should go beyond simply escalating the situation to the IT and legal teams, and should include customer service, public and government relations and employee communications. Board directors, management and the business's various departments all need to understand their role within the overall plan. Multinational corporations must consider reporting requirements and account for additional coordination complexities across regions.

2. Have you tested your preparedness plans?

A table-top simulation allows a business to stress test and improve how it would handle a crisis. This exercise helps companies uncover areas where more preparation is needed. Who should be in charge of these simulations will vary from company to company. But the trials should include high-level participation across the organization, including the CEO. The group has to make sure the simulation incorporates a response that addresses affected stakeholders, taps into all relevant resources and procedures, and points out the unforeseen problems that actions in one department can cause in another.

3. Do customers understand your data collection and usage practices?

You don't want customers to learn about the data you have from a breach notice or media coverage. Instead, your company should periodically evaluate its data collection and uses, and assess how they could be putting the business's reputation at risk. Make sure your data story is clear and that you're articulating the value that the usage provides to customers. Increasingly, organizations are writing their privacy policies with this in mind, clearly outlining what they collect and why.

4. How do you decide how much to invest in security - and where?

One hundred percent security is not possible and the number of possible avenues of attack alone prevents an ironclad defense. In addition, some companies may choose to take on more risk in order to improve the customer experience. In light of this, companies need to weigh the degree of security against the needs of the business. The smartest companies are thinking about security early in the product development cycle. Companies should organize security into tiers, focusing additional resources on the most sensitive data and working outward from there.

5. Are you educating employees on the best cybersecurity practices?

Increasingly, a company's employees are seen as the weakest link in any data security regimen. They are vulnerable to "spear-phishing" attacks, when an email from what appears to be a trusted source – an individual or business – requests secure information about the company. The hope is that the recipient will reply automatically, handing over the keys to the castle in the process. Five out of every six large companies – those with more than 2,500 employees – were hit by spear-phishing attacks in 2014, according to a recent Symantec Internet Security Threat Report. That's a 40 percent increase over the previous year.

To counteract such scams, more companies are choosing to educate employees about common cybersecurity risks. These programs should complement the use of any hard controls, such as mandatory password strength requirements. The goal should be to empower employees by arming them with basic knowledge: how to spot an attempt to breach security, where to go to ask questions, and who to inform when they identify a potential threat.

ILLUSTRATIONS: JUSTIN MEZZELL