Beyond walls

A strong defense is only part of the story, say PwC's DAVID BURG and MEGAN HAAS

A cybersecurity plan should look much the same no matter where you are. After all, the risks for companies are largely the same everywhere in the world.

However, there are some distinctions to be found between regions, notably in Asia. Here, the insider threat can be more serious than elsewhere. In some Asian countries, there is a history of loyalty to family-led companies, but mentorship and other ways to build employee engagement and empowerment are still a small – if growing – part of the business culture. Where loyalty is strong, insider leaks of information are likely to be less common.

Systems and infrastructure haven't kept pace with the explosive front-office growth that we have seen in Asia, leaving security holes that can be exploited. For multinationals, this outdated technology can hamper the execution of an effective global cybersecurity policy. When companies have grown through acquisitions, they may have 15 different kinds of platforms around the world. A standardized system in all offices is essential for consistency in expectations and reporting.

As elsewhere, appointing the right people to boards to handle issues around cybersecurity can be a challenge. There is a global shortage of board members with the necessary expertise and experience, making constructive policy changes, or dealing with a crisis, harder.

Corporate leaders in Asia can be reluctant to share information about breaches which could help other companies be better prepared. Regulations in the region generally don't require disclosure of an incursion, and there is a cultural element – family-dominated enterprises that might want to avoid embarrassment – that inhibits a freer sharing of data breach information.

Still, public disclosures are on the rise. The Hong Kong Monetary Authority is working with the financial services sector to make information regarding incidents available. And we're hearing from Hong Kong-based CIOs that company representatives are cooperating among themselves less formally.

> "Stakeholders value a company more highly if it is able to push past the fear, uncertainty and doubt, to develop a more constructive approach"

DAVID BURG and MEGAN HAAS

David Burg is a Principal in PwC's US Advisory practice based in Virginia. He is the firm's Global and US Cybersecurity Leader. Megan Haas is a Partner at PwC in the firm's Forensic Services team and is based in Hong Kong. Operating in 157 countries, PwC is one of the world's largest professional services firms and one of the top four auditors.

For multinationals operating in Asia, it is important to have a global cybersecurity policy that can then be implemented locally. Tailoring must be done for each region, but realistic minimum security requirements and guidelines on the company's appetite for risk need to be established that apply across the whole firm. Any organization that has a strictly vertical approach on a country-by-country basis is really going to be missing important risks.

In general, companies around the world are moving beyond a strictly defensive posture and starting to see cybersecurity as an asset and a part of a larger strategy that involves the whole business. More are realizing that security by design, at the inception of a product or service, can be a differentiator in the market – a strategic enabler.

In 2015, the World Economic Forum's survey of Fortune 500 CEOs found that cybersecurity was regarded as one of the biggest challenges their companies faced. In at least three Asian economies – Japan, Singapore and Malaysia – a cyber attack was ranked the No. 1 risk for businesses.

In this climate, it has become increasingly clear that stakeholders value a company more highly if it is able to push past the fear, uncertainty and doubt, to develop a more constructive approach. Yet in the minds of too many board members cyber still equals IT. Data security is seen as something very technical, handled by tech folks in the back office.

A global trend among corporations, and even some regulators, is to demand that cyber be a separate component – a peer of IT, reporting directly to the CEO and the board. Currently, data protection is most often under the purview of the chief information officer – strong evidence that it is still viewed as an IT issue. The creation of a new position, a chief information security officer for example, is a really important shift, helping raise the stakes and spread responsibility for data resources throughout the company.

As these challenges are addressed and cybersecurity is integrated into a larger strategy, companies are better able to reap the rewards of collected data used wisely and securely, building trust and creating value.

David Burg and Megan Haas spoke to **JAMAAL MOBLEY**, an Associate in Brunswick's Washington, DC office and part of the Cybersecurity and Privacy practice.