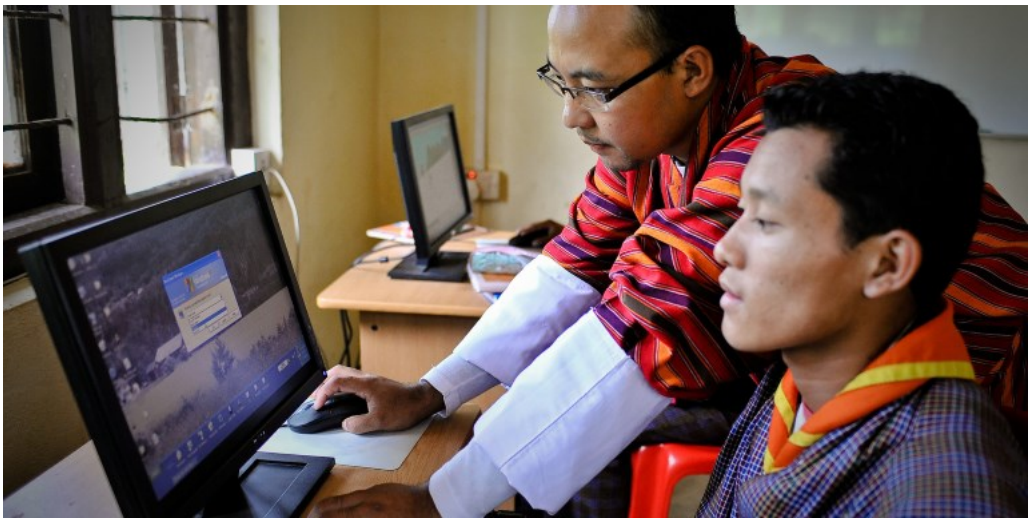
development ASIA
An initiative of Asian Development Bank
sharing development know-how

INSIGHT

One Key Element to Protecting Your Organization from Cyber Crime



Organizations can limit their vulnerability to cyber attacks by being more transparent in how they respond.

Introduction

Asia is an ideal environment for cybercriminals to thrive in due to high digital connectivity and the accelerating pace of digital transformation, contrasted with low cybersecurity awareness, growing cross-border data transfers and evolving but still weak regulations.

Compounding problems is a lack of transparency, which leads to the inaccurate general perception that the cyber threat level is lower in Asia than other regions.

According to the Global Risks Report 2017, concerns around the likelihood and impact of technological threats has sharpened among business executives in Asia, and cyberattacks are ranked among the top five risks of doing business in the region.

Rising cyber risk trends in Asia and key challenges in managing cybersecurity

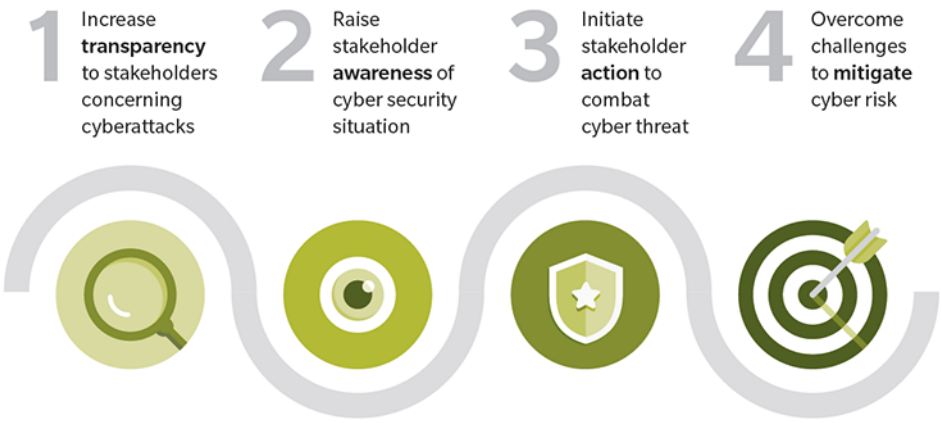
Source: Asia-Pacific Risk Center, "Cyber Risk in Asia-Pacific: The Case for Greater Transparency"

The need to combat cyber threats has never been more urgent in Asia, and many major industries in the region—including construction and engineering, financial, high-tech and electronics—are especially susceptible, according to a new report from Marsh & McLennan Companies' Asia Pacific Risk Center (APRC). A series of recent, high-profile cyberattacks have touched multiple countries and industries across the region, highlighting the issue.

The worrying factor is that although these breaches grab the headlines, there are deeper issues lurking. "The majority of cyberattacks in the region usually go unreported as companies are neither incentivized nor required to do so," said Cheah Wei Ying, an expert on non-financial risk at Oliver Wyman. "This lack of transparency underpins Asia's susceptibility to cyberattacks."

According to the APRC report, raising the transparency level is the first step to cyber risk mitigation, as it leads to higher visibility and greater awareness, necessary to catalyze actions required to mitigate cyber risks.

The role of transparency in mitigating cyber risk



Source: Asia-Pacific Risk Center, "Cyber Risk in Asia-Pacific: The Case for Greater Transparency"

This report was adapted from content featured in BRINK ASIA.

Transparency Trends in Asia

We argue that there is still a lack of transparency in Asia that reduces visibility about the level and frequency of cyber attacks, resulting in the perception that cyber threat is lower in Asia than it actually is. That, in turn, leads to insufficient investment in cybersecurity among corporations and erodes the urgency for tighter cybersecurity among regulators.

The degree to which Asia lags behind the rest of the world is highlighted in recent research, which found the median time between a breach and its discovery for Asian organizations is almost double the global average—172 versus 99 days.

Underpinning the region's transparency issue is its lack of data breach notification laws—which typically require companies that are compromised to inform regulators and stakeholders and take steps to remediate or face a heavy penalty, with the exception of Japan, Australia, South Korea and the Philippines, for example. In some countries, breach notification may be industry-specific; for example, the Monetary Authority of Singapore requires financial institutions to notify them of any breach of security or confidentiality of customer information, or any events that can potentially lead to prolonged service disruption.

This indicates that some governments and policymakers have yet to recognize the importance of transparency in the battle against cyberattacks, which shrouds perceptions and influences the behavior of corporations, resulting in inaction or inadequate mitigation efforts.

Detailed and clear data breach notification laws, supported by enforcement, and a culture of compliance within organizations are critical to improving transparency and improved risk mitigation.

Although this breaks the opacity that most organizations would prefer, such legislation keeps companies accountable to their stakeholders, allowing them to protect their reputations and also minimize losses that could result directly and indirectly from breaches in the cyber architecture.

Another challenge that Asian governments face is that even when willing to put in place legislation to ensure transparency, they have been slow in doing so, compared to the rapid pace of digital transformation in Asia. This is in contrast to the West, where digital progress was slightly more incremental and allowed regulators somewhat more time to adapt, assess and implement necessary safeguards.

Government Actions to Enhance Cyber Transparency

Beyond legislation of detailed and clear data breach notification laws, governments in the region can further mitigate cyber risk through public-private information sharing, the development of cybersecurity knowledge hubs and growing the cybersecurity talent pool.

Public-private information sharing is a useful and necessary defense tool against cyberattacks; both the public and private sector hold critical information in the fight against cybercrime, and there is growing recognition of the need to consolidate this information to obtain a fuller view of the cyber-risk landscape.

Governments should also develop cybersecurity knowledge hubs, which go hand-in-hand with growing the cybersecurity talent pool. Building cyber resilience requires experience and technical expertise, and the development of cybersecurity hubs can act as central knowledge and talent repositories for cutting-edge innovation, technologies and personnel expertise to bridge the gap necessary to build an effective cyber defense.

The Need to Act

Asia has never been more vulnerable to cyber attacks, and the exposure to cyber threat is disproportionately large compared to the amount of investments in cybersecurity and risk management strategies by governments and corporations.

Clearly, a lot more work is required. Governments need to find ways to effectively implement and enforce breach disclosure laws, companies must renew long-entrenched approaches to cybersecurity and individuals have to play their part and practice good cybersecurity habits.

The progress towards transparency is currently piecemeal across stakeholders. The lack of convergence on breach notification regulations in the region suggests that governments have yet to recognize the key role that transparency plays in the fight against cyber risk. That needs to change urgently if the region wants to become more cybersecure.

Resources

Related links

13 Ways to Protect Your NGO from Hacking And Surveillance

Envisioning the Global Financial System in a Decade

Towards a Free, Open and Secure Internet

Meet the experts

Wolfram Hedrich
Executive Director, Asia Pacific Risk Center / Partner, Oliver Wyman's Finance and Risk practice

Wolfram Hedrich is executive director of the Singapore-based Asia Pacific Risk Center. He is also a partner within Oliver Wyman’s Finance and Risk practice.

Follow Wolfram Hedrich on

Jaclyn Yeo
Senior Research Analyst, Asia Pacific Risk Center

Jaclyn Yeo is a senior research analyst at the Singapore-based Asia-Pacific Risk Center and co-author of the Cyber Risk in Asia-Pacific publication. Prior to joining the APRC, she was a risk researcher at the Cambridge Centre for Risk Studies, based in Cambridge, the UK.

Follow Jaclyn Yeo on

Last updated: May 2017