Why Asia Has the Cybersecurity Advantage

By Mikko Niemelä , IDP-C, CEO, Cyber Intelligence House

A new ranking shows how companies around the world are actually faring in the fight to protect data from cybercriminals.

Most Americans were unfamiliar with credit bureau Equifax, before **news** broke of its recent data breach. A large number of the 145 million people potentially affected had never directly supplied information to the company. Equifax receives most of its sensitive information from third parties such as lenders, retailers and debt collectors. How much blame, if any, should these entities bear? Perhaps no one could have anticipated the size and scope of the breach, yet it fits an emerging cybercrime pattern that too many organisations are ignoring.

Today's cybercriminals commonly target the external providers to which companies entrust their data, rather than the companies themselves. For example, months before the world learned of the epic Equifax hack, a subsidiary focused on tax and payroll services suffered a **reportedly unrelated breach**. Increasing automation of business processes has made it easier for hackers to intercept information undetected, even as companies pour **billions of dollars** into cybersecurity.

Cyber Exposure Index

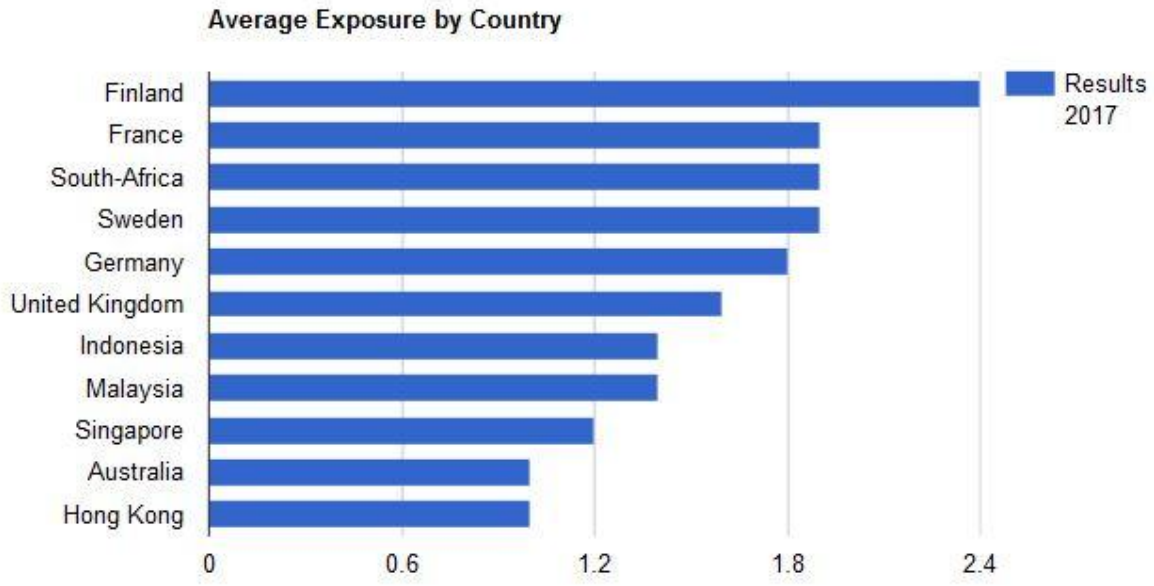
How can I say this with conviction? For years, I have been closely monitoring the corners of the internet where hackers peddle their ill-gotten gains. The information on the dark web and deep web is very temporary – stolen data may appear and vanish forever in a span of five minutes. Therefore, I set out to archive information as and when it appeared. Currently, I have a record of un-indexed web activity that dates back to 2012.

Based upon the last 12 months of illicit online data sharing, I compiled the **Cyber Exposure Index**, which ranks the relative level of exposure among publicly listed firms in 11 countries – Singapore, Finland, South Africa, Australia, Sweden, Germany, the United Kingdom, France, Hong Kong, Malaysia and Indonesia.

I use three criteria to measure cyber exposure:

• Sensitive disclosure – Sensitive information typically consists of internal emails, discussions and confidential matters such as business plans, company valuations and trade secrets.
• Exposed credentials – Usernames, passwords, and their combinations, tokens or other identifiers that enable access to restricted systems.
• Hacker group targeting – The magnitude of coordinated action against a company from international cybercrime networks such as Anonymous.

I assigned each company a score from 1 to 5, reflecting its degree of exposure as compared to the international average. From there, I was able to derive an average score for all 11 countries:



Europe vs. Asia

As you can see, almost all of the most exposed countries are advanced European economies. It might surprise you that digitally mature European organisations have been compromised to a greater extent than those in emerging Asia, which you think would be low-hanging fruit for global hackers.

But I believe Europe’s relative digital maturity actually accounts for its greater overall vulnerability. High labour costs put pressure on European entities to automate processes wherever possible. But removing manual processes and paperwork from the equation heightens opportunities for cyber-theft. When valuable data is stored in a physical file cabinet, there’s virtually no way for a hacker in another country to get at it. Stashing it in the cloud gives cybercriminals a prime target.

Of course, Asia is catching up fast in the digitalisation race. Over the next 6 to 12 months, I expect to see rising cyber-exposure numbers for Asian firms as they continue to close the digital gap. However, Asia has the advantage of late-stage entry. Many European organisations are still encumbered by relatively ineffective and cyber-vulnerable custom tools developed years ago. In Asia, by contrast, digital coming-of-age coincides with easy access to strong off-the-shelf enterprise solutions and reliable communication platforms. This results in working habits that circumvent many of the most vexing areas for cybersecurity.

For example, most of my Asian clients – unlike their European counterparts – prefer to communicate through their personal email instead of their work account. Consequently, their data doesn't end up in easily compromised workplace servers.

Having skipped the most awkward stages of digital adolescence, Asia appears less likely to fall prey to the serious cyber-security lapses that have roiled the West.

Reducing exposure

Outside of dismantling their legacy digital infrastructure and starting from scratch – which might be necessary for some – what can organisations in advanced economies do to limit their cyber-exposure? In my last post, I mentioned how important it is to know what you own as an organisation. Cybersecurity audits should be carried out regularly, with supervision from the board or the C-suite.

In addition, identify your most critical categories of information, and how they might be intercepted – both within and outside your firm's walls. A client once assured me that his most critical data was safely housed on an email server with several layers of protection. "But can you get to it with your mobile phone?" I asked.

"Of course," he said.

"And who else uses your mobile phone?"

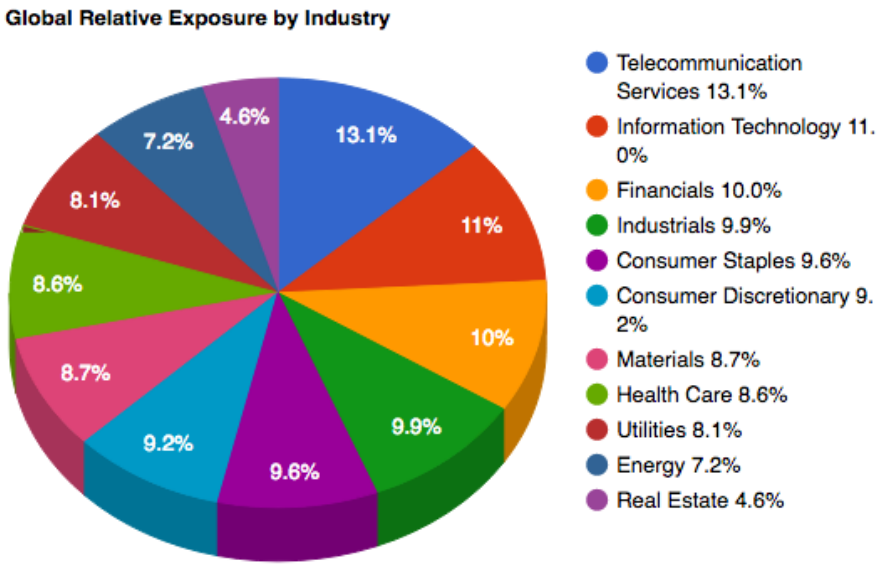
He replied, "My wife, my kids… "

"So the most sensitive data for your whole organisation could potentially be leaked, entirely accidentally, by your family members playing with your phone."

Sadly, a great deal of damaging cyber-exposure begins with wholly gratuitous information sharing. Why would organisations provide more data than necessary to external parties such as payroll vendors? Why give up control over employees' personal information, when an anonymous ID number would suffice? Obviously, more conservative disclosures would have reduced the fallout from the Equifax breach.

The most exposed industries

Though cybersecurity is of concern for all companies, some industries are more squarely in the hackers' crosshairs. The Cyber Exposure Index ranks the most exposed industries across the 11 countries.



Because cybersecurity is a rapidly evolving arena, I plan to prepare a new Cyber Exposure Index every six months. I invite you to **browse the index results** and share them within your organisation.

Mikko S. Niemelä *is president and CEO of Kinkayo, a Singapore-based cyber intelligence agency. He is also chairman of* ***Silverskin*** *and author of* ***Anatomy of a Cyberattack****.*

Follow INSEAD Knowledge on ***Twitter*** *and* ***Facebook****.*

Find article at

https://knowledge.insead.edu/operations/why-asia-has-cybersecurity-advantage

About the author(s)

Mikko Niemelä Mikko S. Niemelä is president and CEO of Cyber Intelligence House.