Seeing Your Firm Through a Hacker's Eyes

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

Cyber-exposure is the best predictor of future hacking activity.

We normally think of hackers as isolated and anti-social – like the hypothetical "genius sitting in bed and playing with his computer" whom Donald Trump surmised might have been behind the 2016 theft of Democratic Party emails. However, cybersecurity experts like myself know that while hackers may not mix well in polite company (at least not openly), their work is highly collaborative, even communal. Without the ability to interact with one another online, hackers would pull off much less cybercrime.

Planning and executing a hack is labour-intensive, and the new generation of hackers tends to be quite wary of wasting time. Rather than starting from scratch, they prefer a process that works much like crowdsourcing. For example, one hacker snatches a cache of encrypted passwords from a

company server and uploads it to the dark web, where it is found by another hacker who excels at decryption. The passwords can then be sold or used for all sorts of sinister purposes by either of the two, or any other hacker who happens across them.

In my experience, a company's current level of cyber-exposure – i.e. how much of its data has already been revealed by and/or to hackers – is the best predictor of the likelihood and intensity of cybercrime activity against that company over the near-to-middle term. It is therefore imperative for companies to know how exposed they are. But this is not easily done, as material may appear on the dark web for only a few minutes – just long enough to sow the seeds of sabotage, which may sprout at any moment thereafter.

Cyber Exposure Index

Since 2016, I have been working with a team of researchers to develop a global cyber-exposure metric applicable to all organisations. Our efforts so far have resulted in the **Cyber Exposure Index** (CEI), which has just been updated for 2018. Based on dark web and deep web activity as well as data breaches from the past 12 months, the CEI ranks the relative exposure of organisations across stock market indices in 11 countries: Australia, Finland, Germany, Hong Kong, Indonesia, Italy, Malaysia, Singapore, South Africa, the United Kingdom and the United States.

The CEI's definition of exposure encompasses disclosure of sensitive information (e.g. internal communications and top-level memoranda), exposed credentials (e.g. usernames, passwords or other information that may allow unauthorised persons to access restricted systems) and hacker group targeting (including coordinated, ideologically motivated attacks by so-called "hacktivists").

SMEs, be on alert

For the latest edition of the CEI, we refined the methodology to account for company size, as measured by number of employees. Adjusting for the fact that larger firms inevitably have more exposure produces fairer and more accurate assessments of risk.

Scrutinising the results through the lens of firm size, a significant gap emerges that should alarm top managers of SMEs. Across countries and

industries, larger companies have far lower levels of relative cyber-exposure on the whole – even though their size would seem to make them a more tempting target for hackers.

Indeed, in this year's CEI, size speaks louder than sector in predicting relative exposure. Surprisingly, differences across industries were nearly negligible by comparison, despite all that we hear about certain industries (energy and finance, for example) being at elevated risk.

The increasingly crowdsourced nature of cyberattacks helps explain this phenomenon. Since most hackers are heading to the dark web for information instead of going straight to the source, smaller, more vulnerable organisations wind up being targeted repeatedly, for the simple reason that their cybersecurity regimes tend to be less robust.

But there is good news here for SMEs. Because latter-day cybercriminals want quick rewards, simply establishing some basic rules and protections could eliminate a company from the list of soft targets. For example, many costly cyberattacks could have been avoided if employees were explicitly prohibited from using their company email addresses to set up personal internet accounts for e-commerce, social media, etc. In a hacker's hands, an employee's email can become an open-sesame for storehouses of valuable online data.

Also, off-the-shelf cybersecurity solutions are becoming better and better. The presence of a standard firewall could be a sufficient deterrent for hackers seeking an easy score.

Know your exposure

How should business leaders read the CEI? I would encourage you to concentrate more on your firm's exposure score than on where you stand relative to competitors. Any level of cyber-exposure – even if it poses no immediate danger – can be damaging for firms, because it will attract more hackers. I liken it to blood in the water. A drop is all it takes to summon the sharks and start a feeding frenzy.

The overarching message for companies, SMEs especially, is to start implementing cybersecurity measures and user awareness training as soon as possible (if you haven't already). Don't be intimidated: It may be less expensive and time-consuming than you think.

Also, put a process in place for monitoring your cyber-exposure. It is the only way to see your own company through a hacker's eyes and thus, the most accurate way to gauge risk and vulnerability.

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

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

Find article at

https://knowledge.insead.edu/operations/seeing-your-firm-through-hackers-eyes

---

About the author(s)

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