Hack to the future: cybersecurity a priority

Late last month, Manny Medina, managing partner of MDM Capital, in a prescient and exquisitely timed move, invested $11 million in Easy Solutions, a fraud protection solutions firm. More than 100 enterprise-class customers, from high-value, client-centric market segments such as banking and online retailers, leverage the Easy Solutions platform to secure over 32 million end users worldwide.

Jerry Haar

At the time of MDM Capital's announcement, it was reported that Chinese hackers have accessed designs for more than two dozen US weapons systems and are the culprits of intellectual property theft of between half and 80% of $300 billion yearly, despite denials by Chinese President Xi Jinping in his recent meeting with President Obama.

Around the same time, too, stories broke in the media about the Department of Justice's search of the email of Fox News journalist James Rosen regarding intelligence leaks about North Korean nuclear tests, and the NSA surveillance program of Americans' phone calls.

In this milieu, cybersecurity has rapidly emerged as a new business priority, given its vital importance in safeguarding intellectual property, financial information and a firm's reputation.

PwC, in conjunction with *CIO* and *CSO* magazines, surveys annually nearly 10,000 global executives to gauge the global state of information security. The most recent survey is illuminating, with 40% of US respondents reporting one or more incidents last year; and the number is rising. The respondents reported financial losses, intellectual property theft, damage, fraud and legal exposure.

The Writer

Jerry Haar is a professor of management and international business at Florida International University and a senior research fellow in the McDonough School of Business at Georgetown University.

Troubling is the disconnect between what executives say and what they do. Asked how confident they were about the effectiveness of their information security activities, 72% answered very confident or somewhat confident. However, 14% of executives surveyed admitted to lacking a strategy and being reactive when it came to information security.

When asked what are the greatest obstacles to improving information security in their companies, the number one response was "resources" – namely, insufficient funding for capital expenditures.

But the answer changed based upon the respondent's position. CEOs agree that lack of capital funding was the problem, but CFOs cite the lack of leadership from the CEO as the reason. CIOs and security executives identify a lack of actionable vision or understanding within the organization as the greatest obstacle.

The PwC survey cites four growing cyberthreats that companies must be made aware of in order to take appropriate cybersecurity measures.

The first is nuisance hacking, such as defacing a firm's website. While not terribly serious, it is annoying to the firm.

The second is hacking for financial gain. This could include not only stealing customer credit card information – something many of us have experienced – but hacking into a company's financial reporting system to obtain earnings reports before they are divulged to the public (profiting by acquiring or selling stock).

A related form is the theft of intellectual property – especially by China, India, Russia and Venezuela. Very often it is state-sponsored espionage.

Finally, a fourth form of cybertheft is "hacktivism" such as WikiLeaks, with the goal of changing or creating a public perception of one's brand or cause.

The principal challenge for companies is to understand that information security is not merely a technology function but a *strategic* function that should report to a senior executive with C-suite reporting responsibility. In fact, it is increasingly common for firms that produce goods and services of a highly proprietary nature to embed security leaders within each business unit, all supporting one another.

As pointed out by Ricardo Villadiego, founder & CEO of Easy Solutions, "The recent $45 million theft, which utilized both online hacking of credit card processors databases in India, and then physical ATM fraud in New York, is just the latest example of why cross-channel fraud protection is increasingly crucial for financial institutions."

To guard against this, companies are adopting a sustained approach to security and taking advantage of newer technologies such as mobile, social media and cloud to drive business growth.

Manny Medina's investment in Easy Solutions is not just a smart business move. It is a harbinger of the shape of things to come in a world where technology for good and technology for evil will continue to clash on an increasingly frequent basis.